Supreme Court, U.S.
FILED

(1) 031565 MAY 14 2004

No. 03- OFFICE OF THE CLERK

In the
Supreme Court of the United States

ALWYN FAREY-JONES
Petitioner,

v.

GEORGE THEOFEL; HOWARD TEIG; DAVID KELLEY; INTEGRATED CAPITAL ASSOCIATES, INC., a Delaware corporation; NANCY RILETT; RYAN TAM; CLAUDIA ENGLISH; TERESA PATTERSON; TANYA YOUNG; ROBERTO MARSELLA; REGINA OVENDEN; EMIL PESIRI; ERIC SULLIVAN; DOUGLAS H. WOLF; and RICHARD BUCKINGHAM,
Respondents.

On Petition for a Writ of Certiorari to the United States Court of Appeals for the Ninth Circuit

PETITION FOR WRIT OF CERTIORARI

ROBERT E. WHITE
Counsel of Record
SUSAN C. RUSHAKOFF
LAW OFFICES OF ROBERT E. WHITE
177 POST STREET, SUITE 890
SAN FRANCISCO, CA 94108
(415) 788-6151

Counsel for Petitioner

Becker Gallagher Legal Publishing, Inc.
800.890.5001

QUESTIONS PRESENTED

The Stored Communications Act, 18 U.S.C. §§ 2701 *et seq*. [hereinafter the "SCA"] is a part of the Electronic Communications Privacy Act of 1986. The SCA protects certain categories of stored e-mail communications and provides for both civil and criminal liability for violation of its provisions. The SCA controls both private access to stored communications and access by law enforcement. This petition for certiorari presents the following questions regarding the interpretation of the SCA:

1. Whether electronic mail ("e-mail") remaining on the server of an Internet Service Provider ("ISP") after it has been read by the user ("post-electronic storage") continues to be subject to the SCA;

2. Whether a determination of gross negligence or even bad faith in a discovery hearing constitutes sufficient *mens rea* to vitiate "authorization" under 18 U.S.C. §§ 2701(c)(1) and (c)(2) of the SCA when the same alleged conduct can be the subject of both civil and criminal penalties;

3. Whether the Court of Appeals' importation of principles of civil trespass law and a dictionary definition of "bad faith" as a basis for vitiating "authorization" under 18 U.S.C. §§ 2701(c)(1) and (c)(2) of the SCA renders these provisions of the SCA unconstitutional as a matter of due process for failure to provide "fair warning" to criminal defendants.

TABLE OF CONTENTS

QUESTIONS PRESENTED i

TABLE OF CONTENTS ii

TABLE OF AUTHORITIES vii

OPINIONS BELOW 1

JURISDICTION 1

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED 1

STATEMENT OF THE CASE 2

- I. OVERVIEW OF THE SCA 2
- II. THE STATUTORY PROVISIONS AT ISSUE . . 3
- III. STATEMENT OF FACTS 5
- IV. PROCEEDINGS IN THE DISTRICT COURT . 7
- V. PROCEEDINGS IN THE COURT OF APPEALS 8
  - A. The Original Opinion of the Court of Appeals 8
    - 1. "Authorization" Under 18 U.S.C. § 2701 8

2. "Electronic Storage" Under 18 U.S.C. § 2510(17)(A) and (B) 10

B. Petition For Rehearing & Amicus Brief of the United States 11

1. "Electronic Storage" 11

2. "Authorization" 13

C. The Court of Appeals' Response To the Petition For Rehearing, Etc. 14

D. The Court of Appeals' Amended Opinion On Denial Of Rehearing 14

1. "Electronic Storage" 14

2. "Authorization" 16

3. Current Status 16

REASONS FOR GRANTING THE PETITION 17

VI. THE COURT OF APPEALS, IN A DECISION OF FIRST IMPRESSION, MISINTERPRETED THE SCA AND THE SCOPE OF "ELECTRONIC STORAGE" 18

A. The Court of Appeals' Construction Of 18 U.S.C. §§ 2510(17)(A) and (B) Fails To Give Effect To Every Word Contained In the Statute 18

B. The Court of Appeals' Construction Of the SCA Is Without Support In the Record 19

C. To the Extent That 18 U.S.C. §§ 2510(17)(A) And (B) Are Ambiguous Or Open To Interpretation, The Court of Appeals Failed To Defer To The Reasonable Judgment Of The Agency Charged With Enforcement Of the Statute 20

D. The Court of Appeals Misread The Legislative History Of The Statute 20

VII. THE COURT OF APPEALS, IN A DECISION OF FIRST IMPRESSION, HAS IGNORED THE "RULE OF LENITY" APPLICABLE TO A CRIMINAL STATUTE AND GREATLY EXPANDED POTENTIAL CIVIL AND CRIMINAL LIABILITY UNDER THE SCA BASED ON INACCURATE COMMON LAW ANALOGIES, AN OUTDATED DICTIONARY DEFINITION OF "BAD FAITH," AND A MISREADING OF THE RECORD BELOW 24

A. The Court of Appeals' Construction of the SCA Violates The Rule of Lenity Applicable To Criminal Statutes 25

B. The Court of Appeals' Use Of Amorphous Common Law Trespass Principles To "Vitiate" The Defense Of Authorization Under The SCA Violates Due Process 26

C. Nothing In The Stored Communications Act Justifies The Use Of Common Law Analogies 26

D. The Court of Appeals Determined That Petitioner Had The Requisite Mens Rea To Violate The SCA By Conflating An Outdated Dictionary Definition Of "Bad Faith" With An Inaccurate Reading Of The Record Below 27

CONCLUSION 30

APPENDIX

Appendix A
Order and Amended Opinion, Ninth Circuit Court of Appeals,
Dated February 17, 2004 . . . . 1a

Appendix B
Opinion, Ninth Circuit Court of Appeals,
Dated August 28, 2003 . . . . 25a

Appendix C
Order Granting Motion to Dismiss, United States District Court for the Northern District of California,
Dated March 8, 2002 . . . . 40a

Appendix D
Order Granting Motions to Quash and Sanctions, United States District Court for the Northern District of California,
Dated February 1, 2002 . . . . 55a

Appendix E
Constitutional and Statutory Provisions Involved . . 66a

Appendix F
Brief for The United States As Amicus Curiae Supporting Defendant/Appellee's Petition For Rehearing And Suggestion For Rehearing En Banc, Filed September 29, 2003, United States Court of Appeals For The Ninth Circuit 73a

TABLE OF AUTHORITIES

CASES

Beck v. Prupis, 529 U.S. 494 (2000) 26, 27

Bifulco v. United States, 447 U.S. 381 (1980) . 13, 25

Bouie v. City of Columbia, 378 U.S. 347 (1964) . . . 26

Fraser v. Nationwide Mutual Ins. Co., 135 F. Supp. 2d 623 (E.D. Pa. 2001), *aff'd on other grounds*, 352 F.3d 107 (3d Cir. 2004) . . 10, 11, 15, 23, 24

Gustafson v. Alloyd Co., 513 U.S. 561 (1995) 21

In re DoubleClick, Inc. Privacy Litigation, 154 F. Supp. 2d 497 (S.D.N.Y. 2001) 10

Lanzetta v. New Jersey, 306 U.S. 451 (1939) 26

Lujan v. Defenders of Wildlife, 504 U.S. 555 (1992) 5

Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002) 2, 11

Nat'l Federation of Federal Employees v. Dep't Of The Interior, 526 U.S. 86 (1999) 20

Reiter v. Sonotone Corp., 442 U.S. 330 (1979) 19

Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F.3d 457 (5th Cir. 1994) 10

United States v. Batchelder, 442 U.S. 114 (1979) . . 25

United States v. Councilman, 245 F. Supp. 2d 319 (D. Mass. 2003) 13, 25

United States v. Harriss, 347 U.S. 612 (1954) 26

United States v. Morton, 467 U.S. 822 (1984) 21

STATUTORY PROVISIONS

18 U.S.C. § 1030, *et seq.* 7
18 U.S.C. § 1030(a)(2)(C) 7
18 U.S.C. § 1962, *et seq.* 27
18 U.S.C. § 2510, *et seq.* 2, 7
18 U.S.C. § 2510(A) 19
18 U.S.C. § 2510(B) 19
18 U.S.C. § 2510(17) 4, 10
18 U.S.C. § 2510(17)(A) . . . . passim
18 U.S.C. § 2510(17)(B) . . . . passim
18 U.S.C. §§ 2701 *et seq.* 1, 7, 8, 21, 23
18 U.S.C. § 2701(a)(1) 4
18 U.S.C. § 2701(a)(2) 4
18 U.S.C. § 2701(b) 5
18 U.S.C. § 2701(b)(1)(A) 4
18 U.S.C. § 2701(b)(1)(B) 5
18 U.S.C. § 2701(b)(2)(A) 5
18 U.S.C. § 2701(b)(2)(B) 5
18 U.S.C. § 2701(c) 7, 21
18 U.S.C. § 2701(c)(1) 17, 30
18 U.S.C. § 2701(c)(2) 17, 30
18 U.S.C. § 2702 . . . . passim
18 U.S.C. § 2702(a)(1) 8, 12
18 U.S.C. § 2702(a)(2) 12, 20, 21, 22
18 U.S.S. § 2702(a)(2)(B) 15

18 U.S.C. § 2703 . . . . 2, 4, 17, 23, 30

18 U.S.C. § 2703(a) 23

18 U.S.C. § 2703(b) 3, 12

18 U.S.C. § 2703(b)(1)(B) 12

18 U.S.C. § 2703(b)(2)(B) 15

18 U.S.C. §2703 (d) 12

18 U.S.C. § 2707 . . . . 2, 4

18 U.S.C. § 2707(c) 4

18 U.S.C. §2711 2

28 U.S.C. § 1254(1) 1

28 U.S.C. § 1331 7

RULES

Fed. R. App. P. 41 16

Fed. R. Civ. P. 12(b)(6) 1, 5, 7

Fed. R. Civ. P. 45(c)(2) 9

Fed. R. Civ. P. 45 (c)(2)(B) 6, 13

Fed. R. Evid. 201(b) 19

LEGISLATIVE MATERIALS

Pub. L. No. 99-508, 100 Stat. 1848 2

Pub. L. No. 107-56, 115 Stat. 272 (October 26, 2001) 2, 23

S. Rep. No. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557 2

H.R. Rep. No. 647, 99th Cong., 2nd Sess. at 65 (1986) 13, 21

H.R. Rep. No. 932, 106th Cong. 2nd Sess. at 7(2000) 13, 22

H.R. Rep. No. 236(I), 107th Cong., 1st Sess. at 57 (2001) 13, 23

OTHER AUTHORITIES

Black's Law Dictionary 139 (6th Ed. 1990) and (7th Ed. 1999) . . . . passim

Prosser & Keaton On the Law Of Torts § 18 (W. Page Keeton ed., 1984) 9, 13

Comment, *Judicial Interpretations Of The Electronic Communications Privacy Act Raise Concerns About Whether The Airline Industries' On-Line Business Ventures Are Protected*, 68 J. Air L. & Com. 819 (Fall 2003) 18

Restatement of the Law of Torts (Second) § 892(B), Comment on Subsection (2) (ALI 1979) 13

Searching and Seizing Computers & Obtaining Electronic Evidence In Criminal Investigations (U.S. Department of Justice, Computer Crime & Intellectual Property Section 2004), http://www.cybercrime.gov/s&smanual2002.htm . . 3

http://www.webopedia.com/TERM/U/URL.html . . 6

U.S. Internet Provider Ass'n, *Electronic Evidence Compliance - A Guide For Internet Service Providers*, 18 Berkeley Tech. L.J. 945 (Fall 2003) 19

PETITION FOR WRIT OF CERTIORARI

Petitioner respectfully prays that a writ of certiorari issue to review the judgment of the United States Court of Appeals in this case.

OPINIONS BELOW

The opinion of the United States Court of Appeals for the Ninth Circuit is reported at 359 F.3d 1066. The previous opinion of the Court of Appeals, issued prior to Petitioner's petition for rehearing and suggestion for rehearing *en banc*, is reported at 341 F.3d 978. The order of the United States District Court for the Northern District of California granting Petitioner's Fed. R. Civ. P. 12(b)(6) motion to dismiss the complaint on March 8, 2002, is not reported.

JURISDICTION

The original opinion of the Court of Appeals was entered on August 28, 2003. The order of the Court of Appeals denying rehearing and amending its opinion on denial of rehearing was entered on February 17, 2004. The jurisdiction of this Court is invoked under 28 U.S.C. § 1254(1).

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

All statutes are set forth in the Appendix at 66a - 72a.

The Stored Communications Act, 18 U.S.C. §§ 2701 et seq.

Sec. 2701. - Unlawful access to stored communications

Sec. 2702. - Voluntary disclosure of customer communications or records

Sec. 2703. - Required disclosure of customer communications or records

Sec. 2510. - Definitions

Sec. 2707. - Civil action

Sec. 2711 - Definitions for chapter

STATEMENT OF THE CASE

I. OVERVIEW OF THE SCA

The SCA was enacted by Congress in 1996 as part of the Electronic Communications Privacy Act [hereinafter the "ECPA"]. See Pub. L. No. 99-508, 100 Stat. 1848. The purpose of the ECPA was to afford privacy protection to electronic communications. Title I of the ECPA amended the federal Wiretap Act, which previously addressed only wire and oral communications, to "address[ ] the interception of ... electronic communications." S.Rep. No. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557. Title II of the ECPA created the SCA, which was designed to "address[ ] access to stored wire and electronic communications and transactional records." *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir. 2002). Both the Wiretap Act and the SCA were more recently amended by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (the USA PATRIOT Act), Pub.L. No. 107- 56, 115 Stat. 272 (October 26, 2001). *Id.*

The SCA governs civil conduct as well as circumscribing the activities of law enforcement when electronic information is sought in criminal cases and investigative matters. *See Searching and Seizing Computers & Obtaining Electronic Evidence In Criminal Investigations* (U.S. Dep't of Justice, Computer Crime & Intellectual Property Section 2004).[1]

Thus decisions concerning the reach of the SCA have implications far beyond civil cases – they have a direct impact on the activities of law enforcement. Brief of the United States As Amicus Curiae Supporting Defendant/Appellee's Petition For Rehearing & Suggestion For Rehearing En Banc, filed Sept. 29, 2003 [hereinafter "Government's Amicus Brief," reproduced in full in the Appendix ("App.")], at App. 79a - 80a, 82a (decision below has caused prosecutors in the Ninth Circuit to stop using 18 U.S.C. § 2703(b) to compel disclosure of stored communications and has potential national implications due to the location of some of the nation's largest e-mail providers within the jurisdiction of the Ninth Circuit).

II. THE STATUTORY PROVISIONS AT ISSUE

The SCA prohibits access "without authorization" to a wire or electronic communication while it is in "electronic storage" in "a facility through which an electronic communication service is provided" (18 U.S.C.A.

---

[1] This publication is commonly known as the "Search & Seizure Manual." It can be found on the website of the Computer Crime & Intellectual Property Section either in HTML format at the following Universal Resource Locator (URL): http://www.cybercrime.gov/s&smanual2002.htm) or in Adobe .pdf format at the following location: http://www.cybercrime.gov/s&smanual2002.pdf.

§ 2701(a)(1)), or access intentionally gained in excess of such "authorization" (*Id.* § 2701(a)(2)).

> "Electronic storage" is defined in 18 U.S.C. § 2510(17) as
>
> (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
> (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication; . . . .

The defined term "electronic storage" is also used in 18 U.S.C. § 2703, which regulates government access to stored communications, and section 2702, which regulates voluntary disclosure by network service providers of customer communications and records both to government and non-governmental entities.

Violations of the SCA can be the subject of both civil and criminal sanctions. 18 U.S.C. § 2707 provides for a civil remedy that includes injunctive relief in appropriate cases, actual damages,[2] punitive damages for intentional violations, and a reasonable attorney's fee. The criminal sanction for violation of the Stored Communications Act can be as much as five years in prison for a first offense if the violation is found to have been committed "for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act," plus a fine. 18 U.S.C. § 2701(b)(1)(A). Imprisonment for a repeat offense can be as much as ten years. *Id.* § 2701(b)(1)(B). For less egregious violations, the statute provides for fine and imprisonment up to one year for a first offense and up to five years for a repeat violation. *Id.* § 2701(b)(2)(A) and (b)(2)(B). Criminal offenses under the Act arise from the same conduct that is governed by its civil provisions. *See* 18 U.S.C. § 2701(b). Thus the same issues tendered in a civil defense of "authorization" are an affirmative defense to a criminal charge of violation of the Stored Communications Act.

---

[2] Section 2707(c) provides for minimum damages of $1,000 where actual damages cannot be shown.

III.STATEMENT OF FACTS[3]

On September 25, 2001, Petitioner's former counsel, Iryna A. Kwasny, issued a subpoena *duces tecum* out of the United States District Court for the Northern District of California to NetGate Internet ("NetGate") for certain electronic and other documents maintained by NetGate as part of its Internet and e-mail service for Respondents. The subpoena was issued in aid of an action pending in the United States District Court for the Eastern District of New York between Petitioner and three of the Respondents (the "New York Action"). The subpoena sought production of "[a]ll copies of emails sent or received by anyone" at the domain name of "ica-ipg.com." As mandated by Fed. R. Civ. P. 45(c)(2)(B), the subpoena expressly advised Netgate of its right to move to quash on a variety of grounds, including privilege, undue burden and disclosure of trade secrets. Order Granting [Petitioner's] Motion to Dismiss, App. 45a, n.4.

---

[3] This section of the petition is derived from Respondents' Complaint in the District Court and the order of the Magistrate Judge granting the motion of certain Respondents to quash or modify the subpoena *duces tecum* issued on behalf of defendant. The latter is reproduced at App. 55a. Inasmuch as plaintiffs' Complaint was dismissed as a result of defendant's Fed. R. Civ. P. 12(b)(6) motion, to the extent that the facts as set forth in this section are based on the Complaint filed in the District Court, they were assumed, for purposes of the motion only, to be true. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992).

The subpoena was thereafter served on NetGate and counsel for two of the Respondents. Within a few days of receiving the subpoena, NetGate produced a "sampling" of some electronic documents (the "NetGate Data") "by uploading the data to the NetGate website and then delivering to attorney Kwasny the URL[[4]] that was necessary to access and view the information." Ms. Kwasny provided the URL to Petitioner. The NetGate Data was later provided to counsel for defendants Buckingham and Wolf in the course of discovery in the New York Action – they were not notified contemporaneously of the access given to Kwasny and Petitioner by Netgate.

Upon learning that their e-mails had been accessed, the defendants in the New York action moved to quash or modify the subpoena *duces tecum* in the Northern District of California and obtained a stay of the return date of the subpoena pending hearing on their motion.

While the motion to quash was pending, on November 8, 2001, Respondents filed a civil action in the United States District Court for the Northern District of California against Petitioner and Kwasny alleging violations of the Wiretap Act, the SCA, and the Computer Fraud & Abuse Act, 18 U.S.C. § 1030(a)(2)(c) (the "CFAA"), in addition to pendent state law claims. The factual predicate of the civil action was the access described above gained by Petitioners and Kwasny to Respondents' e-mails.

---

[4] "URL" is an abbreviation for "Uniform Resource Locator," the global address of documents and other resources on the World Wide Web portion of the Internet. See "(Webopedia) The #1 Online Encyclopedia Dedicated to Computer Technology," (http://www.webopedia.com/TERM/U/URL.html).

On February 1, 2002, while Farey-Jones' motion to dismiss the Complaint below was pending, the Magistrate Judge quashed the subpoena, finding that the subpoena was "grossly overbroad" and that the communications sought were likely to contain information that was "obviously irrelevant, and/or sensitive commercially (trade secrets) or personally, and/or privileged." The Magistrate Judge further concluded that the crafting of the subpoena was done with "at least gross negligence" and that defendants' course of conduct taken as a whole was in bad faith. Sanctions totaling $9,250.00 were awarded against defendants Farey-Jones and Kwasny and Farey-Jones' New York counsel. Order Granting Motions To Quash & Sanctions, App. 55a - 65a.

IV. PROCEEDINGS IN THE DISTRICT COURT

Jurisdiction in the District Court was based on 28 U.S.C. § 1331 (federal question jurisdiction), 18 U.S.C. 2701 *et seq.* (the SCA), 18 U.S.C. § 1030, *et seq.* (the Computer Fraud & Abuse Act), and 18 U.S.C. § 2510 *et seq.* (the Wiretap Act). Petitioner's Fed. R. Civ. P. 12(b)(6) motion to dismiss the Complaint was granted on March 8, 2002. Order Granting Motion To Dismiss, App. 40a - 52a. The District Court rejected Respondents' SCA claim, holding that Netgate had authorized access to the e-mails that are the subject of the Complaint and that the exception contained in 18 U.S.C. § 2701(c) therefore applied. The District Court rejected

Respondents' claim under 18 U.S.C. § 2702(a)(1), holding that section 2702 applied to the ISP (Netgate) and not to Petitioner.

The District Court rejected Respondents' Wiretap Act claims, holding that the Wiretap Act only applied to contemporaneous communications. The District Court rejected Respondents' CFAA claims because the Complaint revealed that Petitioner had not accessed Respondents' computers as distinguished from those of Netgate, and because Respondents had not alleged any compensable damages under the CFAA. Having disposed of all of Respondents' federal claims, the District Court exercised its discretion not to consider the pendent state law claims.[5]

V. PROCEEDINGS IN THE COURT OF APPEALS

A. The Original Opinion Of the Court of Appeals

1. "Authorization" Under 18 U.S.C. § 2701

The Court of Appeals for the Ninth Circuit (B. Fletcher, Kozinski and Trott, JJ) reversed and remanded. App. 25a - 39a . The court held that since the term "authorization" under the SCA was not defined, it would interpret "authorization" by analogy to the general law of trespass and cases determining whether landowner consent to a disputed entry was invalidated by deception on the part of the alleged trespasser. *Id.* at 29a. The court observed that certain types of knowing deceit could undermine consent although it acknowledged that "[t]hese are fine and sometimes incoherent distinctions." *Id.* at 30a. The court concluded that Netgate's authorization was vitiated by the overbroad subpoena because, unbeknownst to Netgate, the subpoena was "invalid." *Id.* at 31a. The court concluded that Petitioner and his former counsel had at least constructive knowledge of the subpoena's invalidity because of its extreme overbreadth, its complete non-compliance with the Federal Rules, and the Magistrate Judge's order, which the court viewed as a finding that defendants "acted in bad faith *and* with gross negligence in drafting and deploying" the subpoena (emphasis supplied). *Id.* at 31a.[6] While acknowledging that the authority on which it principally relied (*Prosser & Keaton On the Law Of Torts* § 18, at 119 (W. Page Keeton ed., 5th ed. 1984) [hereinafter *"Prosser & Keaton"*] stated that constructive knowledge of a mistake is only "probably sufficient" to vitiate consent, it concluded that the gross negligence *and* bad faith in the instant case was sufficient. *Id.* at 32a n2.

---

[5] In a subsequent order, the District Court dismissed the Complaint against attorney Kwasny on the same grounds. Respondents' appeals from the District Court's orders of dismissal were thereafter consolidated.

The court regarded the Fed. R. 45(c)(2) recitals of the deponent's rights to resist the subpoena as a "good start," but disagreed with the District Court that they reduced or diminished any claim of coercion of the deponent, due to the cost involved in contesting a subpoena, the coercive effect of a subpoena and the potential lack of financial interest of a third party in objecting. *Id.* at 33a.

---

[6] The Magistrate Judge did *not* find that the issuance of the subpoena, as such, was in "bad faith," characterizing it as "at least gross negligence." Order Granting Motions To Quash & Sanctions, App. 62a. While the Magistrate Judge did find that the course of conduct, taken as a whole, constituted "bad faith," the overwhelming majority of that conduct followed the issuance of the subpoena and its service on Netgate. *Id.*

2. "Electronic Storage" Under 18 U.S.C. § 2510(17)(A) and (B)

Since the District Court had ruled that Netgate had authorized the access, the District Court did not address Petitioner's alternative argument that the e-mails in question were not in "electronic storage" as that term is defined in 18 U.S.C. § 2510(17) and were therefore outside the coverage of the SCA. The Court of Appeals reached the issue and concluded that even e-mails that had already been read, but which remained on the ISP's server, were nevertheless still in "electronic storage." *Id.* at 33a - 35a. The court acknowledged that two federal district courts had reached the contrary conclusion,[7] based on the definition of "electronic storage" contained in 18 U.S.C. § 2510(17)(A),[8] and that the Fifth Circuit had concluded to the contrary in connection with messages stored on a computer bulletin board system.[9]

The Court of Appeals came to its conclusion based on the definition of "electronic storage" contained in 18 U.S.C.

---

[7] *In re DoubleClick, Inc. Privacy Litigation*, 154 F. Supp. 2d 497, 511-12 (S.D.N.Y. 2001); *Fraser v. Nationwide Mutual Ins. Co.*, 135 F. Supp. 2d 623, 635-36 (E.D. Pa. 2001) [*aff'd on other grounds*, 352 F.3d 107 (3d Cir. 2004)] [hereinafter "*Fraser*"].

[8] "[A]ny temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof."

[9] *Steve Jackson Games, Inc. v. U.S. Secret Service*, 36 F.3d 457, 461-62 (5th Cir. 1994).

§ 2510(17)(B).[10] It concluded that it was "obvious" that the messages remained on the ISP's server as "backup" for the benefit of the user and therefore came under this definition of "electronic storage." The court rejected the contrary conclusion of the District Court in *Fraser*.

The court affirmed the dismissal of the Wiretap Act claim based on *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002), which held that the Wiretap Act applies only to "'acquisition contemporaneous with transmission.'" App. at 36a. The court reversed the dismissal of the CFAA claim without leave to amend, concluding that the District Court erred by reading an ownership or control requirement into the statute. *Id.* at 36a - 37a.

The Court of Appeals rejected Petitioner's remaining arguments and, in light of its reversal of the federal claims, reinstated the state law claims. *Id.* at 39a.

B. Petition For Rehearing & Amicus Brief Of The United States

1. "Electronic Storage"

Petitioner sought rehearing and suggested rehearing *en banc*. He was joined by the United States on the issue of whether e-mails remaining on the ISP's server after being read by the user were in "electronic storage." App. at 73a - 99a. In its amicus curiae brief, the Government observed that the decision of the Court of Appeals largely nullified 18

---

[10] "[A]ny storage of such communication by an electronic communication service for purposes of backup protection of such communication."

U.S.C. § 2703(b), the portion of the SCA that governs law enforcement access to electronic communications when not in "electronic storage." App. at 79a. The Government contended that the Court of Appeals' interpretation of "electronic storage" ignored the plain language of the statutory definitions and in particular the fact that the definition of "backup" contained in 18 U.S.C. § 2510(17)(B) refers to backups of "*such* communication[s]," i.e. the "temporary, intermediate" communications referred to in section 2510(17)(A). *Id.* at 83a - 84a (emphasis supplied). The Government pointed out that by taking so expansive a view of "electronic storage," the court rendered sections 2702(a)(2) and 2703(b) of the SCA superfluous since, under the court's formulation, *any* communication stored by an electronic communications service is in "electronic storage." *Id.* at 85a - 87a. The Government also observed that the court's misreading of section 2510(17)(A) and (B) effectively eliminated the SCA's carefully drawn distinction between communications in "electronic storage" in an "electronic communications service" and those stored in a "remote computing service," another defined term in the SCA. *See* 18 U.S.C. § 2703(B)(1)(B) and App. at 87a. The Government viewed the distinction as critical since communications in "electronic storage" for 180 days or less are accessible to law enforcement only by a search warrant whereas communications stored on a "remote computing service" are disclosable pursuant to subpoena or court order under 18 U.S.C. § 2703(d). *Id.* at 88a. The Government contended that the court's misconstruction had a similar impact on section 2702(a)(1) and (a)(2), which govern voluntary disclosure of communications by network service providers. *Id.* at 89a. As a result, the Government concluded that the court's misconstruction of section 2510(17)(A) and (B) created "an unprecedented impediment for law enforcement access to stored communications." *Id.* at 82a. As the

Government also stated, "the significance of this change for law enforcement cannot be overstated." *Id.* at 93a.

The Government also contended that the court's decision ignored the legislative history of the SCA. *Id.* at 93a - 95a, citing H.R. Rep. No. 647, 99th Cong., 2nd Sess., at 65 (1986), H.R. Rep. No. 932, 106th Cong., 2nd Sess. at 7 (2000); and H.R. Rep. No. 236(I), 107th Cong., 1st Sess. at 57 (2001) (USA PATRIOT Act).

2. "Authorization"

In addition to addressing the Court of Appeals' misconstruction of section 2510(17)(A) and (B), Petitioner also contended that the court's elastic use of civil trespass analogies to "vitiate" otherwise valid authorization in the instant case had the further impact of criminalizing a much broader spectrum of conduct. Petitioner pointed out that such a holding is contrary to the "rule of lenity" that requires that criminal statutes be construed narrowly. *See Bifulco v. United States*, 447 U.S. 381, 387 (1980); *United States v. Councilman*, 245 F. Supp. 2d 319, 320-21 (D. Mass. 2003) (applying rule to a case arising under the SCA). Petitioner also questioned how a facially valid subpoena issued under the auspices of the District Court containing the notices specified by Fed. R. Civ. P. 45(c)(2)(B) could be treated as having no legal or practical significance whatsoever.

Petitioner also examined the substantive applicability of the civil trespass analogies relied upon by the court. Petitioner noted that each required *actual knowledge of the falsity of the representation* to vitiate otherwise valid consent. *See Prosser & Keaton, supra*, § 18 at 120; *Restatement of the Law of Torts (Second)* § 892B, Comment on Subsection (2) (ALI 1979). Petitioner further noted that the authorities relied upon did not support the court's conclusion that constructive knowledge was sufficient to vitiate consent.

C. The Court of Appeals' Response To the Petition For Rehearing, Etc.

The Court of Appeals ordered the amicus curiae brief of the United States filed on September 29, 2003. On October 1, 2003, the court ordered a response from Respondents, limited to the issues raised by the United States in its amicus curiae brief. Respondents filed their responsive brief on October 22, 2003.

D. The Court Of Appeals' Amended Opinion On Denial Of Rehearing

On February 17, 2004, six months after the petition for rehearing was filed, the Court of Appeals denied the petition for rehearing and rejected the suggestion for rehearing *en banc*. It also amended its opinion to address some of the issues raised by the Government and by Petitioner.

1. "Electronic Storage"

The Court of Appeals rejected the Government's interpretation of Section 2510(17)(A), concluding as a matter of grammar that the reference to "such communication" referred to "a wire or electronic communication" and not to the type of storage ("temporary, intermediate storage . . .") Amended Opinion, App. at 17a. The court also held that the interpretation offered by the Government would rob section 2510(17)(B) of meaning because, in its view, virtually any backup of a message in "temporary, intermediate" storage would itself be in "temporary, intermediate" storage. *Id.* at 18a. In response to the Government's contention that only the underlying e-mail message need be in "temporary, intermediate" storage, the court stated that, in its view,[11] the lifespan of a backup was necessarily tied to that of the underlying message. It stated that once the "underlying message has expired [sic.] in the normal course, any copy is no longer performing any backup function." *Id.* Therefore an ISP that kept permanent copies of such temporary messages, in the court's view, could not be fairly described as "backing up" such messages. *Id.*

The court rejected the Government's argument that the court's interpretation of the SCA was structurally anomalous. It did so because it could see instances where storage of an electronic communication would not be for backup purposes nor in "temporary, intermediate" storage. *Id.* at 18a. The court similarly concluded that since remote computing services and electronic communications services are often, but not invariably, the same entities, instances could occur where files could be subject to the more liberal rules of access provided by section 2702(a)(2)(B) and 2703(b)(2)(B) without triggering the more stringent requirements pertaining to e-mail backups under the court's interpretation of section 2510(17)(B). *Id.* at 18a - 19a. The court dismissed the legislative history offered by the Government as either consistent with the court's reading of the statute, of little probative value, or issued under the misapprehension that the district court decision in *Fraser* correctly stated the law. Acknowledging that its interpretation of the SCA differed from that of the Government, the court nevertheless adhered to its view that prior access was irrelevant to whether the messages at issue were in electronic storage. *Id.* at 20a.

---

[11] There is no evidence in the record that would support *any* of the factual conclusions stated in this portion of the Court of Appeals' opinion.

2. "Authorization"

In response to Petitioner's petition for rehearing on this issue, the court acknowledged that since the SCA defines a criminal defense and includes an explicit *mens rea* requirement, a defendant cannot be charged with a violation of the SCA based on constructive knowledge. App. at 13a, n.2. "Rather, the defendant must have consciously procured consent through improper means." *Id.* The court noted that the Magistrate Judge had held that the defendants had "acted in bad faith," which, in its view, satisfied the *mens rea* requirement. *Id.* It cited to *Black's Law Dictionary* 139 (6th Ed. 1990) and its definition of "bad faith" as "not simply bad judgment or negligence, but . . . conscious doing of a wrong because of dishonest purpose or moral obliquity" to conclude that the Magistrate Judge's finding established the requisite *mens rea*. *Id.* The Court amended its opinion accordingly, denied rehearing and rejected the suggestion for rehearing *en banc*.[12]

3. Current Status

Petitioner filed a motion in the Court of Appeals seeking to stay issuance of mandate pending filing of the instant Petition pursuant to Fed. R. App. P. 41 and Ninth Circuit Rule 41-1 on the grounds that the court's opinion raised "at least two issues that present substantial questions potentially meriting further review in the Supreme Court . . ." The

---

[12] The court's order further provided that no additional petitions for rehearing would be entertained.

Court of Appeals granted the motion by order filed March 4, 2004.

REASONS FOR GRANTING THE PETITION

The Court of Appeals' misconstruction of the SCA in this case has seriously impeded law enforcement activities by (1) holding that e-mails in "post electronic storage" are subject to section 2701(c)(1) and (c)(2) of the SCA and (2) requiring search warrants to gain access to e-mails to which the Government has previously gained access either by subpoena or court order pursuant to section 2703.

The Court of Appeals' misconstruction of the SCA also exposes whole classes of citizens to potential criminal liability for accessing e-mails in "post electronic storage" and does so by the application of inapposite legal principles designed for civil trespass cases and an outdated *Black's Law Dictionary* definition of "bad faith" that provides no clear guidance as to what conduct is and is not proscribed. Expansion of potential criminal liability of the SCA thus both violates the constitutionally-mandated "rule of lenity" requiring narrow construction of criminal statutes and also deprives potential defendants of the "fair warning" that due process mandates before criminal penalties can be imposed.

The Court of Appeals' misconstruction of the SCA is inconsistent with the plain text of the statute, ignores the integrated structure of the SCA's various provisions, finds no support in and is contrary to the extensive legislative history, and ignores the deference to which the Government is entitled in reasonably construing a statute that it is charged to administer. The constitutional and other infirmities in the Court of Appeals' decision in a case of first impression and with nationwide implications can and should be corrected by this Court.

VI. THE COURT OF APPEALS, IN A DECISION OF FIRST IMPRESSION, MISINTERPRETED THE SCA AND THE SCOPE OF "ELECTRONIC STORAGE"

A. The Court Of Appeals' Construction Of 18 U.S.C. §§ 2510(17)(A) and (B) Fails To Give Effect To Every Word Contained In the Statute

The decision of the Court of Appeals represents the first decision by a federal appeals court regarding the definition of "electronic storage" under the SCA and whether e-mails that remain on the server of the ISP after being read are or are not in "electronic storage." This aspect of the court's opinion has already been the subject of criticism. Comment, *Judicial Interpretations Of The Electronic Communications Privacy Act Raise Concerns About Whether The Airline Industries' On-Line Business Ventures Are Protected, 68 J. Air L. & Com.* 819, 839 n.126 (Fall 2003):

> Backup protection excluding post-transmission storage under subsection (B) is *not* equivalent to temporary intermediate storage in subsection (A) because subsection (B) includes the additional limitation of pertaining to storage provided by an electronic communication service. . . Theofel fails to recognize this distinction. (emphasis supplied)

See 18 U.S.C. § 2510(17)(B): "[A]ny storage of *such communication by an electronic communication service* for purposes of backup protection of *such communication* . . .

(emphasis supplied)." The second use of "such communication" is the point of distinction that the Court of Appeals overlooked and which Petitioner and the United States consistently urged below. It is a basic canon of statutory construction that every word in a statute is to be given meaning. *Reiter v. Sonotone Corp.*, 442 U.S. 330, 339 (1979). The interpretation given to section 2510(A) and (B) by the Court of Appeals fails to follow this basic rule. The result has been a major retrenchment on the part of the Government regarding the scope of the SCA and its ability to gain access to e-mails as part of its law enforcement activities. U.S. Internet Service Provider Ass'n, *Electronic Evidence Compliance - A Guide For Internet Service Providers, 18 Berkeley Tech. L.J.* 945, 961 (Fall 2003); Government's Amicus Brief (App. 79a - 80a, 82a).

B. The Court Of Appeals' Construction Of The SCA Is Without Support In the Record

The Court of Appeals rejected the Government's structural argument regarding the reach of the SCA because it could conceive of instances where storage of an electronic communication would not be for backup purposes nor in "temporary, intermediate" storage. It did so entirely without benefit of any record evidence nor even citation to authority. To the extent the court was relying on its own experience regarding the Internet, such experience cannot be the substitute for judicial notice. Fed. R. Evid. 201(b).

C. To the Extent That 18 U.S.C. §§ 2510(17)(A) And (B) Are Ambiguous Or Open To Interpretation, The Court of Appeals Failed To Defer To The Reasonable Judgment Of The Agency Charged With Enforcement Of The Statute

The Court of Appeals ignored another basic rule of statutory construction. When a statute is silent or ambiguous, courts *must* defer to a reasonable construction by the agency charged with implementation of the statute, in this case the Justice Department. *Nat'l Federation of Federal Employees v. Dep't Of The Interior*, 526 U.S. 86, 92 (1999). The Court of Appeals in the instant case, in denying rehearing, explicitly acknowledged that it disagreed with the Justice Department's long-standing interpretation of the SCA provisions regarding "electronic storage."

D. The Court of Appeals Misread The Legislative History Of The Statute

The drafters of the SCA explicitly considered what would happen when a recipient of e-mail kept a copy of the e-mail on the ISP's server after receipt:

> Sometimes the addressee, having requested and received a message, chooses to leave it in storage on the service for re-access at a later time. The Committee intends that, in leaving the message in storage, the addressee should be considered the subscriber or user from whom the system received the communication for storage, *and that such communication should continue to be covered by section 2702(a)(2).*

H.R. Rep. No. 647, 99th Cong., 2nd Sess., at 65 (1986) (emphasis added). See Government's Amicus Brief, App. 93a - 94a. Section 2702(a)(2) refers to communications that are stored on a "remote computing service," which are not communications in "electronic storage" under section 2701.

The Court of Appeals dismissed this reference to legislative history because the cited discussion addressed the issue of what constituted "remote computing services" and did not explicitly address what constituted "electronic storage." App. at 19a. In so doing the court ignored the interrelationship between the various parts of the SCA and the fundamental canon of construction requiring that a statute be construed harmoniously so that its constituent provisions are each taken into account. *See, e.g., United States v. Morton*, 467 U.S. 822, 828 (1984); *Gustafson v. Alloyd Co.*, 513 U.S. 561, 575 (1995).

The court's statement that use of the word "continue" (in "continue to be covered by section 2702(a)(2)") supported its reading of the statute is also not borne out by context. H.R. Rep. No. 647 discussed the then proposed enactment of the SCA and did so as a whole, discussing sections 2701 and 2702 (and other sections of the statute) together. See H.R. Rep. No. 647 at 65:

> In the case of either *electronic mail* or voice mail, the sender - a user of the service - has necessarily authorized the addressee's access to the message. *The addressee's acquisition of the message is therefore clearly within the contemplation of section 2701(c).* Sometimes the addressee, having requested and received a message, chooses to leave it in storage on the service for re-access at a later time. *The Committee intends that, in leaving the message in*

> *storage, the addressee should be considered the subscriber or user from whom the system received the communication for storage, and that such communication should continue to be covered by section 2702(a)(2).* (emphasis supplied)

The court interpreted "continue" as indicating a non-exclusive mode of protection for a certain category of electronic communications. App. at 19a. This again ignores the integrated nature of the SCA and construes section 2702 in isolation.

The Court of Appeals also rejected the Government's citation to H.R. Rep. No. 932, 106th Cong. at 7 (2000). See App. at 19a - 20a. As the Government pointed out, in 2000, Congress *rejected* a proposed amendment that would have expanded the definition of electronic storage to include "any storage of an electronic communication by an electronic communications service *without regard to whether the communication had been accessed by the intended recipient*" (see Government Amicus Brief, App. 94a). The court's response was that "[t]his sort of legislative history has very little probative value; Congress *might* have rejected the amendment precisely because it thought the definition already applied." App. at 19a - 20a (emphasis supplied).

The court's statement that "[t]his sort of legislative history has very little probative value; . . ." was unaccompanied by authority. It is also unsupported by logic. The far more persuasive inference is that the amendment was rejected because of a legislative determination not to change existing law. It is sheer speculation to conclude that an amendment was rejected because it was declarative of existing law. Moreover, if the definition "already applied" as the Court of Appeals speculates, its application would be entirely consistent with the distinction drawn by Petitioner and the Government between "electronic storage" and "remote computing services."

The court then disposed of the Government's reference to H.R. Rep. No. 236(I), 107th Cong., at 57 (2001) (the House Report on the USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 272 (2001)). See Government's Amicus Brief (App. 95a):

> In the course of discussing an amendment to the SCA allowing for nationwide service of § 2703(a) warrants, the [H.R. Rep. No. 236(I)] states that "2703(a) requires a search warrant to compel service providers to disclose *unopened* e-mails."

The Court of Appeals concluded that this portion of H.R. Rep. No. 236(I) addressed an "unrelated issue and merely assumes that the definition only applies to unopened e-mail." App. at 20a. It also dismissed this remark as a "natural [assumption] given that *Fraser* had recently been decided." *Id.*

An examination of H.R. Rep. No. 236(I) does not bear out the Court of Appeals' dismissal of this portion of the legislative history. The USA PATRIOT Act amended many provisions of the SCA. *See, e.g.,* Section 102 of the Act (seizure of voicemails pursuant to warrants), changes to the definitions contained in 18 U.S.C. §§ 2510, *including a ministerial change to 18 U.S.C. § 2510(17)(A)*, as well as sections 2702 and 2703. The close relationship between sections 2701, 2702 and 2703 of the Stored Communications Act is demonstrated by the PATRIOT Act amendments themselves. The Court of Appeals' assumption that the legislative history was premised upon Congressional knowledge of the decision by the district court in *Fraser*, decided in March of 2001, is improbable to the point of speculation and in any event is supported nowhere in the voluminous legislative history of the USA PATRIOT Act.

As demonstrated above, the Court of Appeals' dismissal of the Government's presentation of the legislative history of the SCA cannot withstand analysis.

VII. THE COURT OF APPEALS, IN A DECISION OF FIRST IMPRESSION, HAS IGNORED THE "RULE OF LENITY" APPLICABLE TO A CRIMINAL STATUTE AND GREATLY EXPANDED POTENTIAL CIVIL AND CRIMINAL LIABILITY UNDER THE SCA BASED ON INACCURATE COMMON LAW ANALOGIES, AN OUTDATED DICTIONARY DEFINITION OF "BAD FAITH," AND A MISREADING OF THE RECORD BELOW

In concluding that Petitioner's access to Respondents' e-mails violated the SCA, the Court of Appeals initially held that even constructive knowledge would justify the imposition of civil liability. App. at 31a - 33a. In response to Petitioner's rehearing petition, the court agreed with Petitioner that constructive knowledge could not be sufficient due to the "explicit *mens rea* requirement" contained in the SCA. App. at 13a, n.2. Instead it held that a defendant would have to be shown to have "consciously procured consent through improper means." *Id.* The Court of Appeals resorted to a *Black's Law Dictionary* definition to equate a finding of "bad faith" by a discovery magistrate with "conscious doing of a wrong because of dishonest purpose or moral obliquity." *Id.*, *citing Black's Law Dictionary* 139 (6th Ed. 1990). In so doing, the Court of Appeals misapplied the common law principles it relied upon to "vitiate" consent of the ISP, inaccurately read the record of the proceedings before the Magistrate Judge to equate the negligent issuance of a subpoena with "bad faith," conflated "bad faith" with conscious wrongdoing, and thereby expanded the coverage of a criminal statute in violation of the "rule of lenity" and fundamental principles of due process.

A. The Court of Appeals' Construction of the SCA Violates The Rule of Lenity Applicable To Criminal Statutes

It is settled beyond dispute that criminal statutes are narrowly construed. "[A]mbiguities in criminal statutes must be resolved in favor of lenity." *United States v. Batchelder*, 442 U.S. 114, 121 (1979)[13]. This "rule of lenity" applies both to interpretations of the substantive reach of criminal prohibitions and to the penalties they impose. *See Bifulco v. United States*, 447 U.S. 381, 387 (1980). It has been applied to the definition of "electronic storage" contained in the SCA. *United States v. Councilman*, 245 F. Supp. 2d 319, 320-21 (D. Mass. 2003). The Court of Appeals erred in applying expansive civil theories of tort liability to what is also a criminal statute, thereby extending its reach in violation of this cardinal rule of statutory construction. The court's action is all the more troubling since, as discussed below, the court is penalizing Petitioner and his former counsel based on an inaccurate reading of the record below and the conflation of an outdated and ambiguous dictionary definition of "bad faith" with conscious knowledge of wrongdoing.

---

[13] As noted previously, violations of the provisions of the SCA that are the subject of this Petition can give rise to both civil and criminal penalties. The same conduct and the same affirmative defenses, including the defense of "authorization," apply to both. See section II, *supra*.

B. The Court of Appeals' Use Of Amorphous Common Law Trespass Principles To "Vitiate" The Defense Of Authorization Under The SCA Violates Due Process

The Court of Appeals' decision to use common law trespass analogies to give a gloss to the SCA also violates a related principle of criminal law. It exposes persons to criminal liability based on a doctrine of vitiated consent that the Court of Appeals itself acknowledged is grounded in confusing if not downright "incoherent" distinctions arising under the common law of trespass. App. at 12a. Due process requires that a criminal statute give fair warning of the circumstances giving rise to a violation and the imposition of criminal penalties. *See, e.g., United States v. Harriss*, 347 U.S. 612, 617 (1954); *Lanzetta v. New Jersey*, 306 U.S. 451 (1939); *see also Bouie v. City of Columbia*, 378 U.S. 347 (1964). Engrafting a doctrine of vitiated consent based on amorphous principles of civil trespass law clearly does not satisfy the requirements of due process in addition to violating the "rule of lenity."

C. Nothing In The Stored Communications Act Justifies The Use Of Common Law Analogies

The authority upon which the Court of Appeals relied to import civil trespass principles into the SCA does not support the extension. *Beck v. Prupis*, 529 U.S. 494, 500-01 (2000), cited by the Court of Appeals (see App. at 10a), used common law conspiracy principles to give a gloss to the Racketeer Influenced & Corrupt Organizations Act, 18 U.S.C. §§ 1962 *et seq.*, because "Congress use[d] language with a settled meaning at common law." *Id.* at 500. This Court found the common law to be the "obvious" source for the meaning of the provisions in the RICO statute at issue in *Beck*. *Id.* It found the underlying legal principle "so widely accepted at the time of RICO's adoption as to be incorporated in the common understanding of 'civil conspiracy.'" *Id.* at 504.

There is no similar basis in the ECPA or the SCA justifying resort to tort/trespass principles. The Court of Appeals points to no legislative or other history justifying its doing so.

D. The Court of Appeals Determined That Petitioner Had The Requisite Mens Rea To Violate The SCA By Conflating An Outdated Dictionary Definition Of "Bad Faith" With An Inaccurate Reading Of The Record Below

To satisfy the *mens rea* requirement of the SCA, the Court of Appeals relied upon a purported finding by the Magistrate Judge that Petitioner and his former counsel had acted in "bad faith." App. at 13a, n.2. It then cited *Black's Law Dictionary* 139 (6th Ed. 1990) and its definition of "bad faith" as "not simply bad judgment or negligence, but . . . conscious doing of a wrong because of dishonest purpose or moral obliquity" to determine that the *mens rea* requirement had been satisfied. *Id.*

The first problem with the Court of Appeals' use of a dictionary definition of "bad faith" is that *Black's Law*

Dictionary defines "bad faith" as encompassing many kinds of different conduct, including conduct that *clearly* does not rise to "conscious doing of a wrong because of dishonest purpose or moral obliquity." Here is the full definition as contained in the current edition of *Black's* (not the one relied upon by the Court of Appeals):

> **bad faith,** *n*. **1.** Dishonesty of belief or purpose <the lawyer filed the pleading in bad faith>. -- Also termed *mala fides* (**mal-< <**schwa**> >-fi-deez**). "A complete catalogue of types of bad faith is impossible, but the following types are among those which have been recognized in judicial decisions: evasion of the spirit of the bargain, lack of diligence and slacking off, willful rendering of imperfect performance, abuse of a power to specify terms, and interference with or failure to cooperate in the other party's performance." Restatement (Second) of Contracts § 205 cmt. d (1981). **2.** *Insurance*. An insurance company's unreasonable and unfounded (though not necessarily fraudulent) refusal to provide coverage in violation of the duties of good faith and fair dealing owed to an insured. * Bad faith often involves an insurer's failure to pay the insured's claim or a claim brought by a third party. **3.** An insured's claim against an insurance company for an unreasonable and unfounded refusal to provide coverage. -- **bad-faith,** *adj*. Cf. GOOD FAITH.

Black's Legal Dictionary (7th ed. 1999) (emphasis supplied).

Not only does the current definition of the "bad faith" contained in *Black's* no longer contain the language relied upon by the Court of Appeals, but the definition makes clear that not all "bad faith" rises to the level of intentional conduct described by the Court of Appeals as fulfilling the SCA's *mens rea* requirement (*i.e.*, "the defendant must have consciously procured consent through improper means"). The dictionary definition of the term includes lack of diligence, evasion, failure to cooperate, and unreasonable and unfounded (though not necessarily fraudulent) behavior, wholly aside from the authors' recognition that the term cannot even be definitively catalogued. Under both the "rule of lenity" and the commands of due process, a legal standard that equates an ambiguous dictionary definition (and a changing one at that) with an explicit *mens rea* requirement clearly cannot pass constitutional muster.

The second problem with the Court of Appeals' resort to the Magistrate Judge's discovery order is that the Magistrate Judge did *not* conclude that *the subpoena* was necessarily obtained in "bad faith." In one instance the Magistrate Judge characterized the issuance of the subpoena as "at least gross negligence." Order Granting Motions To Quash & Sanctions, App. 62a. Elsewhere the Magistrate Judge referred to the subpoena as "thoughtlessly crafted" and "unreasonable." *Id.* at 58a. While the Magistrate Judge did find that the course of conduct, taken as a whole, constituted "bad faith," the overwhelming majority of that conduct followed the issuance of the subpoena and its service on Netgate. *Id.* at 62a.

This is not a lawsuit about bad faith. The issue tendered by Petitioner's motion to dismiss was whether access to the e-mails was "authorized" or not. The sole basis for the Court of Appeals' concluding that Netgate's consent was "vitiated" was the alleged deceit resulting from "bad faith" procurement of the subpoena. Not only is that term ambiguous to the point of constitutional infirmity in the context of this case, but the factual predicate is missing as well.

Both as a matter of the constitutionally-permissible construction of a criminal statute and as a factual matter, the Court of Appeals' use of ambiguous civil trespass analogies and an outmoded dictionary definition to give a gloss to the meaning of the term "authorization" under 18 U.S.C. § 2701(c)(1) and (c)(2) (and by implication sections 2702 and 2703 of the SCA) also cannot withstand scrutiny.

CONCLUSION

This case presents issues of first impression regarding the construction of the SCA. The Court of Appeals misconstrued the statute and did so in a manner that impacts severely the ability of law enforcement to protect our citizens in these extremely troubled times. It also engrafted a confusing and constitutionally infirm test for determining when a key exception to the coverage of the SCA applies. For all of the foregoing reasons the petition should be granted.

Respectfully submitted,

ROBERT E. WHITE
Counsel of Record
SUSAN C. RUSHAKOFF
LAW OFFICES OF ROBERT E. WHITE
177 Post Street, Suite 890
San Francisco, CA 94108
Telephone: (415) 788-6151

Dated MAY 14, 2004

APPENDIX A

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

No. 02-15742
D.C. No.
CV-01-04166-MMC

GEORGE THEOFEL; HOWARD TEIG; DAVID KELLEY; INTEGRATED CAPITAL ASSOCIATES, INC., A Delaware Corporation; NANCY RILETT; RYAN TAM; CLAUDIA ENGLISH; TERESA PATTERSON; TANYA YOUNG; ROBERTO MARSELLA; REGINA OVENDEN; EMIL PESIRI; ERIC SULLIVAN; DOUGLAS H. WOLF; RICHARD BUCKINGHAM,
Plaintiffs -Appellants,

v.

ALWYN FAREY-JONES; IRYNA A. KWASNY,
Defendants-Appellees.

No. 02-15742
D.C. No.
CV-01-04166-MMC

GEORGE THEOFEL; HOWARD TEIG;)
DAVID KELLEY; INTEGRATED)
CAPITAL ASSOCIATES, INC., A)
Delaware Corporation; NANCY)
RILETT; RYAN TAM; CLAUDIA)
ENGLISH; TERESA PATTERSON;)
TANYA YOUNG; ROBERTO)
MARSELLA; REGINA OVENDEN; EMIL)
PESIRI; ERIC SULLIVAN; DOUGLAS H.)
WOLF; RICHARD BUCKINGHAM,)
Plaintiffs-Appellants,)
)
v.)
)
ALWYN FAREY-JONES; IRYNA A.)
KWASNY,)
Defendants-Appellees.)
)

No. 03-15301
D.C. No.
CV-01-04166-MMC

ORDER AND AMENDED OPINION

Appeal from the United States District Court for the
Northern District of California
Maxine M. Chesney, District Judge, Presiding

Argued and Submitted
April 2, 2003-San Francisco, California

Filed August 28, 2003
Amended February 17, 2004

Before: Betty B. Fletcher, Alex Kozinski and Stephen S. Trott, Circuit Judges.

Opinion by Judge Kozinski

ORDER

The opinion filed on August 28, 2003, shall be amended as follows.

Replace footnote 2 at slip op. 12343 with:

> Prosser and Keeton say that a plaintiff's consent is probably invalid if the defendant "ought to have known in the exercise of reasonable care" about the mistake. *Prosser & Keeton* § 18, at 119. Because the Stored Communications Act defines a criminal offense and includes an explicit mens rea requirement, *see* 18 U.S.C. § 2701(a)(1), we do not think a defendant can be charged with constructive knowledge on a showing of mere negligence. Rather, the defendant must have consciously procured consent through improper means. In this case, the magistrate found that defendants had acted in bad faith. That is enough to charge them with knowledge of NetGate's mistake. *See* Black's Law Dictionary 139 (6th ed. 1990) (defining "bad faith" as "not simply bad judgment or negligence, but . . . conscious doing of a wrong because of dishonest purpose or moral obliquity").

Replace the second paragraph at slip op. 12346 with:

> The United States, as amicus curiae, disputes our interpretation. It first argues that, because subsection

(B) refers to "any storage of *such* communication," it applies only to backup copies of messages that are themselves in temporary, intermediate storage under subsection (A). The text of the statute, however, does not support this reading. Subsection (A) identifies a type of communication ("a wire or electronic communication") and a type of storage ("temporary, intermediate storage . . . incidental to the electronic transmission thereof"). The phrase "such communication" in subsection (B) does not, as a matter of grammar, reference attributes of the type of storage defined in subsection (A). The government's argument would be correct if subsection (B) referred to "a communication in such storage," or if subsection (A) referred to a communication in temporary, intermediate storage rather than temporary, intermediate storage of a communication. However, as the statute is written, "such communication" is nothing more than shorthand for "a wire or electronic communication."

The government's contrary interpretation suffers from the same flaw as *Fraser's*: It drains subsection (B) of independent content because virtually any backup of a subsection (A) message will itself qualify as a message in temporary, intermediate storage. The government counters that the statute requires only that the underlying message be temporary, not the backup. But the lifespan of a backup is necessarily tied to that of the underlying message. Where the underlying message has expired in the normal course, any copy is no longer performing any backup function. An ISP that kept permanent copies of temporary messages could not fairly be described as "backing up" those messages.

The United States also argues that we upset the structure of the Act by defining "electronic storage" so broadly as to be superfluous and by rendering irrelevant certain other provisions dealing with remote computing services. The first claim relies on the argument that any copy of a message necessarily serves as a backup to the user, the service or both. But the mere fact that a copy *could* serve as a backup does not mean it is stored for that purpose. We see many instances where an ISP could hold messages not in electronic storage--for example, e-mail sent to or from the ISP's staff, or messages a user has flagged for deletion from the server. In both cases, the messages are not in temporary, intermediate storage, nor are they kept for any backup purpose.

Our interpretation also does not render irrelevant the more liberal access standards governing messages stored by remote computing services. *See* 18 U.S.C. §§ 2702(a)(2), 2703(b). The government's premise is that a message stored by a remote computing service "solely for the purpose of providing storage or computer processing services to [the] subscriber," *id.* §§ 2702(a)(2)(B), 2703(b)(2)(B), would also necessarily be stored for purposes of backup protection under section 2510(17)(B), and thus would be subject to the more stringent rules governing electronic storage. But not all remote computing services are also electronic communications services and, as to those that are not, section 2510(17)(B) is by its own terms inapplicable. The government notes that remote computing services and electronic communications services are "often the same entities," but "often" is not good enough to make the government's point. Even as to remote computing services that are also electronic communications services, not air storage covered by sections 2702(a)(2)(B) and 2703(b)(2)(B) is also covered by section 2510(17)(B). A remote computing service might be the only place a user stores his messages; in that case, the messages are not stored for backup purposes.

Finally, the government invokes legislative history. It cites a passage from a 1986 report indicating that a committee intended that messages stored by a remote computing service would "continue to be covered by section 2702(a)(2)" if left on the server after user access. H.R. Rep. No. 647, 99th Cong., at 65 (1986). The cited discussion addresses provisions relating to remote computing services. We do not read it to address whether the electronic storage provisions also apply. *See id.* at 64-65. The committee's statement that section 2702(a)(2) would "continue" to cover e-mail upon access supports our reading. If section 2702(a)(2) applies to e-mail even before access, the committee could not have been identifying an exclusive source of protection, since even the government concedes that unopened e-mail is protected by the electronic storage provisions.

The government also points to a subsequent, rejected amendment that would have made explicit the electronic storage definition's coverage of opened e-mail. *See* H.R. Rep. No. 932, 106th Cong., at 7 (2000). This sort of legislative history has very little probative value; Congress might have rejected the amendment precisely because it thought the definition already applied.

Finally, the government points to a passing reference in another recent report. H.R. Rep. No. 236(I), 107th Cong., at 57 (2001). The discussion addresses an unrelated issue and merely assumes that the definition only applies to unopened e-mail. This assumption was natural given that *Fraser* had recently been decided.

We acknowledge that our interpretation of the Act differs from the government's and do not lightly conclude that the government's reading is erroneous. Nonetheless, for the reasons above, we think that prior access is irrelevant to whether the messages at issue were in electronic storage. Because plaintiff's e-mail messages were in electronic storage regardless of whether they had been previously delivered, the district court's decision cannot be affirmed on this alternative ground.[4]

The petition for rehearing and rehearing en banc is otherwise DENIED. *See* Fed. R. App. P. 35; Fed. R. App. P. 40. No further petitions will be accepted.

---

[4] Defendants urge us to affirm on the additional ground that the complaint at one point alleges they "access[ed] . . . *Plaintiffs'* computer systems through which electronic communications systems are provided." Resp. Br. of Def./Appellee at 16 (emphasis added), Plaintiffs' computers, they note, are not "facilities" covered by 18 U.S.C. § 2701(a)(1). *Id.* at 15. We construe complaints liberally, however, *see Lynn v. Sheet Metal Workers' Int'l Ass'n*, 804 F.2d 1472, 1482 (9th Cir. 1986), and the substance of plaintiffs' claims is that defendants improperly accessed *Net-Gate's* servers.

OPINION

KOZINSKI, Circuit Judge:

We consider whether defendants violated federal electronic privacy and computer fraud statutes when they used a "patently unlawful" subpoena to gain access to e-mail stored by plaintiffs' Internet service provider.

Background

Plaintiffs Wolf and Buckingham, officers of Integrated Capital Associates, Inc. (ICA), are embroiled in commercial litigation in New York against defendant Farey-Jones. In the course of discovery, Farey-Jones sought access to ICA's e-mail. He told his lawyer Iryna Kwasny to subpoena ICA's ISP, NetGate.

Under the Federal Rules, Kwasny was supposed to "take reasonable steps to avoid imposing undue burden or expense" on NetGate. Fed. R. Civ. P. 45(c)(1). One might have thought, then, that the subpoena would request only e-mail related to the subject matter of the litigation, or maybe messages sent during some relevant time period, or at the very least those sent to or from employees in some way connected to the litigation. But Kwasny ordered production of "[a]ll copies of emails sent or received by anyone" at ICA, with no limitation as to time or scope.

NetGate, which apparently was not represented by counsel, explained that the amount of e-mail covered by the subpoena was substantial. But defendants did not relent. NetGate then took what might be described as the "Baskin-Robbins" approach to subpoena compliance and offered defendants a "free sample" consisting of 339 messages. It posted copies of the messages to a NetGate website where, without notifying opposing counsel, Kwasny and Farey-Jones read them. Most were unrelated to the litigation, and many were privileged or personal.

When Wolf and Buckingham found out what had happened, they asked the court to quash the subpoena and award sanctions. Magistrate Judge Wayne Brazil soundly roasted Farey-Jones and Kwasny for their conduct, finding that "the subpoena, on its face, was massively overbroad" and "patently unlawful," that it "transparently and egregiously" violated the Federal Rules, and that defendants "acted in bad faith" and showed "at least gross negligence in the crafting of the subpoena." He granted the motion to quash and socked defendants with over $9000 in sanctions to cover Wolf and Buckingham's legal fees. Defendants did not appeal that award.

Wolf, Buckingham and other ICA employees whose e-mail was included in the sample also filed this civil suit against Farey-Jones and Kwasny. They claim defendants violated the Stored Communications Act, 18 U.S.C. § 2701 *et seq.*, the Wiretap Act, 18 U.S.C. § 2511 *et seq.*, and the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, as well as various state laws. The district court held that none of the federal statutes applied, and dismissed the claims without leave to amend. It declined jurisdiction over the state law claims under 28 U.S.C. § 1367(c)(3). Plaintiffs now appeal.

Analysis

1. The Stored Communications Act provides a cause of action against anyone who "intentionally accesses without authorization a facility through which an electronic communication service is provided . . . and thereby obtains,

alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage." 18 U.S.C. §§ 2701(a)(l), 2707(a), "[E]lectronic storage" means either "temporary, intermediate storage . . . incidental to . . . electronic transmission," or "storage . . . for purposes of backup protection." *Id.* § 2510(17). The Act exempts, inter alia, conduct "authorized . . . by the person or entity providing a wire or electronic communications service," *id.* § 2701(c)(1), or "by a user of that service with respect to a communication of or intended for that user," *id.* § 2701(c)(2).

The district court dismissed on the ground that NetGate had authorized defendants' access. It held that this consent was not coerced, because the subpoena itself informed NetGate of its right to object. Plaintiffs contend that NetGate's authorization was nonetheless invalid because the subpoena was patently unlawful. Their claim turns on the meaning of the word "authorized" in section 2701. We have previously reserved judgment on this question, *see Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 879 n.8 (9th Cir. 2002), while other circuits have considered related issues, *see, e.g., EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577,582 n. 10 (lst Cir. 2001) (holding access might be "unauthorized" under the Computer Fraud and Abuse Act if it is "not in line with the reasonable expectations" of the party granting permission (internal quotation marks omitted)); *United States v. Morris*, 928 F.2d 504, 510 (2d Cir. 1991) (holding access unauthorized where it is not "in any way related to [the system's] intended function").

We interpret federal statutes in light of the common law. *See Beck v. Prupis*, 529 U.S. 494, 500-01 (2000). Especially relevant here is the common law of trespass. Like the tort of trespass, the Stored Communications Act protects individuals' privacy and proprietary interests. The Act reflects Congress's judgment that users have a legitimate interest in the confidentiality of communications in electronic storage at a communications facility. Just as trespass protects those who rent space from a commercial storage facility to hold sensitive documents, *cf. Prosser and Keeton on the Law of Torts* § 13, at 78 (W. Page Keeton ed., 5th ed. 1.984), the Act protects users whose electronic communications are in electronic storage with an ISP or other electronic communications facility.

A defendant is not liable for trespass if the plaintiff authorized his entry. *See Prosser & Keeton* § 13, at 70. But "an overt manifestation of assent or willingness would not be effective . . . if the defendant knew, or probably if he ought to have known in the exercise of reasonable care, that the plaintiff was mistaken as to the nature and quality of the invasion intended." *Id.* § 18, at 119; *cf. Restatement (Second) of Torts* §§ 173, 892B(2). Thus, the busybody who gets permission to come inside by posing as a meter reader is a trespasser. *J.H. Desnick, M.D., Eye Servs., Ltd. v. ABC*, 44 F.3d 1345, 1352 (7th Cir. 1995). So too is the police officer who, invited into a home, conceals a recording device for the media. *Cf. Berger v. Hanlon*, 129 F.3d 505, 516-17 (9th Cir. 1997), *vacated*, 526 U.S. 808 (1999), *reinstated in relevant part*, 188 F.3d 1155, 1157 (9th Cir. 1999).

Not all deceit vitiates consent. "[T]he mistake must extend to the essential character of the act itself, which is to say that which makes it harmful or offensive, rather than to some collateral matter which merely operates as an inducement." *Prosser & Keeton* § 18, at 120 (footnote omitted). In other words, it must be a "substantial mistake[ ] . . . concerning the nature of the invasion or the extent of the harm." *Restatement (Second) of Torts* § 892B(2) cmt. g. Unlike the phony meter reader, the restaurant critic who poses as an ordinary customer is not liable for trespass, *Desnick*, 44 F.3d at 1351; nor, unlike the wired cop, is the invitee who conceals only an intent to repeat what he hears, *cf. Dietemann v. Time, Inc.*, 449 F.2d 245, 249 (9th Cir. 1971) (invasion of privacy claim). These results hold even if admission would have been refused had all the facts been known.

These are fine and sometimes incoherent distinctions. *See Med. Lab. Mgmt. Consultants v. ABC*, 30 F. Supp. 2d 1182, 1201-04 (D. Ariz. 1998), *aff'd*, 306 F.3d 806 (9th Cir. 2002). But the theory is that some invited mistakes go to the essential nature of the invasion while others are merely collateral. Classification depends on the extent to which the intrusion trenches on "the specific interests that the tort of trespass seeks to protect." *Desnick*, 44 F.3d at 1352; *see also Lewis v. United States*, 385 U.S. 206, 211 (1966); *Food Lion, Inc. v. Capital Cities/ABC, Inc.*, 194 F.3d 505, 517-18 (4th Cir. 1999).

We construe section 2701 in light of these doctrines. Permission to access a stored communication does not constitute valid authorization if it would not defeat a trespass claim in analogous circumstances. Section 2701 (c)(1) therefore provides no refuge for a defendant who procures consent by exploiting a known mistake that relates to the essential nature of his access.

Under this standard, plaintiffs have alleged facts that vitiate NetGate's consent, NetGate disclosed the sample in response to defendants' purported subpoena. Unbeknownst to NetGate, that subpoena was invalid. This mistake went to the essential nature of the invasion of privacy. The subpoena's falsity transformed the access from a bona fide state-sanctioned inspection into private snooping. *See Restatement (Second) of Torts* § 174 (addressing "consent induced by fraud or mistake as to the validity of purported legal authority"); *cf. Bumper v. North Carolina*, 391 U.S. 543, 549 (1968) ("A search conducted in reliance upon a warrant cannot later be justified on the basis of consent if it turns out that the warrant was invalid."). The false subpoena caused disclosure of documents that otherwise would have remained private; it effected an "invasion . . . of the specific interests that the [statute] seeks to protect." *Desnick*, 44 F.3d at 1352.

Defendants had at least constructive knowledge of the subpoena's invalidity. It was not merely technically deficient, nor a borderline case over which reasonable legal minds might disagree. It "transparently and egregiously" violated the Federal Rules, and defendants acted in bad faith and with gross negligence in drafting and deploying it.[1] They are charged with knowledge of its invalidity. *See Prosser & Keeton* § 18, at 119 (consent likely vitiated where defendants "ought to have known in the exercise of reasonable care" of the mistake).[2]

---

[1] Defendants had a full and fair opportunity to litigate the validity and good faith of the subpoena in the sanctions proceedings. Those proceedings were filed as a miscellaneous action on a separate docket from both the underlying New York litigation and the instant suit; defendants did not appeal. The magistrate's findings are therefore preclusive. *Cf.* 18 James Win. Moore et al., *Moore's Federal Practice* § 132.03[4][k][vii], at 132126 (3d ed. 1997) (judgment of contempt is issue preclusive); 3 Ronald E. Malten & Jeffrey M. Smith, Legal Malpractice § 21.14, at 286 (5th ed. 2000) (attorney disciplinary proceedings may be issue preclusive).

[2] Prosser and Keeton say that a plaintiff's consent is probably invalid if the defendant "ought to have known in the exercise of reasonable care" about the mistake. *Prosser & Keeton* § 18, at 119.

That NetGate could have objected is immaterial. The subpoena may not have been coercive, but it was deceptive, and that is an independent ground for invalidating consent. *See Restatement (Second) of Torts* § 892B(2)-(3). It was a piece of paper masquerading as legal process. NetGate produced the sample in response and doubtless would not have done so had it known the subpoena was void--particularly in light of its own legal obligation not to disclose such messages to third parties, *see* 18 U.S.C. § 2702(a)(1). That NetGate could have objected proves disclosure was not an inevitable consequence, but it was still a foreseeable one (and the intended one).

Allowing consent procured by known mistake to serve as a defense would seriously impair the statute's operation. A hacker could use someone else's password to break into a mail server and then claim the server "authorized" his access. Congress surely did not intend to exempt such intrusions—indeed, they seem the paradigm of what it sought to prohibit. *Cf. Morris*, 928 F.2d at 510 (access gained by guessing someone else's password is not "authorization" under the Computer Fraud and Abuse Act).

Because the Stored Communications Act defines a criminal offense and includes an explicit mens rea requirement, *see* 18 U.S.C. § 2701(a)(1), we do not think a defendant can be charged with constructive knowledge on a showing of mere negligence. Rather, the defendant must have consciously procured consent through improper means. In this ease, the magistrate found that defendants had acted in bad faith. That is enough to charge them with knowledge of NetGate's mistake. *See* Black's Law Dictionary 139 (6th ed. 1990) (defining "bad faith" as "not simply bad judgment or negligence, but . . . conscious doing of a wrong because of dishonest purpose or moral obliquity").

The subpoena power is a substantial delegation of authority to private parties, and those who invoke it have a grave responsibility to ensure it is not abused. Informing the person served of his right to object is a good start, *see* Fed. R. Civ. P. 45(a)(1)(D), but it is no substitute for the exercise of independent judgment about the subpoena's reasonableness. Fighting a subpoena in court is not cheap, and many may be cowed into compliance with even overbroad subpoenas, especially if they are not represented by counsel or have no personal interest at stake. Because defendants procured consent by exploiting a mistake of which they had constructive knowledge, the district court erred by dismissing based on that consent.

Defendants ask us to affirm on the alternative ground that the messages they accessed were not in "electronic storage" and therefore fell outside the Stored Communications Act's coverage. *See* 18 U.S.C. § 2701(a)(1). The Act defines "electronic storage" as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." *Id.* § 2510(17), *incorporated by id.* § 2711 (1). Several courts have held that subsection (A) covers e-mail messages stored on an ISP's server pending delivery to the recipient. *See In re Doubleclick, Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 511-12 (S.D.N.Y. 2001); *Fraser v. Nationwide Mut, Ins. Co.*, 135 F. Supp. 2d 623, 635-36 (E.D. Pa. 2001); *cf. Steve Jackson Games, Inc. v. U.S. Secret Serv.*, 36 F.3d 457, 461-62 (5th Cir. 1994) (messages stored on a BBS pending delivery). Because subsection (A) applies only to messages in "temporary, intermediate storage," however, these courts have limited that subsection's coverage to messages not yet delivered to their intended recipient. *See Doubleclick*, 154 F. Supp. 2d at 512; *Fraser*, 135 F. Supp. 2d at 636.

Defendants point to these cases and argue that messages remaining on an ISP's server after delivery no longer fall within the Act's coverage. But, even if such messages are not within the purview of subsection (A), they do fit comfortably within subsection (B). There is no dispute that messages remaining on NetGate's server after delivery are stored "by an electronic communication service" within the meaning of 18 U.S.C. § 2510(17)(B). *Cf. Doubleclick*, 154 F. Supp. 2d at 511 (holding that subsection (B) did not apply because the communications at issue were not being stored by an electronic communication service). The only issue, then, is whether the messages are stored "for purposes of backup protection." 18 U.S.C. § 2510(17)(B). We think that, within the ordinary meaning of those terms, they are,

An obvious purpose for storing a message on an ISP's server after delivery is to provide a second copy of the message in the event that the user needs to download it again--if, for example, the message is accidentally erased from the user's own computer. The ISP copy of the message functions as a "backup" for the user. Notably, nothing in the Act requires that the backup protection be for the benefit of the ISP rather than the user. Storage under these circumstances thus literally fails within the statutory definition.[3]

---

[3] That defendants did not read the messages until NetGate posted them to a website is immaterial. Defendants' unlawful subpoena caused Net-Gate to retrieve the messages from electronic storage and make them available. That constitutes "access" within the meaning of the Act.

One district court reached a contrary conclusion, holding that "backup protection" includes only temporary backup storage pending delivery, and not any form of "post-transmission storage." *See Fraser*, 135 F. Supp. 2d at 633-34, 636. We reject this view as contrary to the plain language of the Act. In contrast to subsection (A), subsection (B) does not distinguish between intermediate and post-transmission storage. Indeed, *Fraser's* interpretation renders subsection (B) essentially superfluous, since temporary backup storage pending transmission would already seem to qualify as "temporary, intermediate storage" within the meaning of subsection (A). By its plain terms, subsection (B) applies to backup storage regardless of whether it is intermediate or post-transmission.

The United States, as amicus curiae, disputes our interpretation. It first argues that, because subsection (B) refers to "any storage of *such* communication," it applies only to backup copies of messages that are themselves in temporary, intermediate storage under subsection (A). The text of the statute, however, does not support this reading. Subsection (A) identifies a type of communication ("a wire or electronic communication") and a type of storage ("temporary, intermediate storage . . . incidental to the electronic transmission thereof"). The phrase "such communication" in subsection (B) does not, as a matter of grammar, reference attributes of the type of storage defined in subsection (A). The government's argument would be correct if subsection (B) referred to "a communication in such storage," or if subsection (A) referred to a communication in temporary, intermediate storage rather than temporary, intermediate storage of a communication. However, as the statute is written, "such communication" is nothing more than shorthand for "a wire or electronic communication."

The government's contrary interpretation suffers from the same flaw as *Fraser's:* It drains subsection (B) of independent content because virtually any backup of a subsection (A) message will itself qualify as a message in temporary, intermediate storage. The government counters that the statute requires only that the underlying message be temporary, not the backup. But the lifespan of a backup is necessarily tied to that of the underlying message. Where the underlying message has expired in the normal course, any copy is no longer performing any backup function. An ISP that kept permanent copies of temporary messages could not fairly be described as "backing up" those messages.

The United States also argues that we upset the structure of the Act by defining "electronic storage" so broadly as to be superfluous and by rendering irrelevant certain other provisions dealing with remote computing services. The first claim relies on the argument that any copy of a message necessarily serves as a backup to the user, the service or both. But the mere fact that a copy *could* serve as a backup does not mean it is stored for that purpose. We see many instances where an ISP could hold messages not in electronic storage—for example, e-mail sent to or from the ISP's staff, or messages a user has flagged for deletion from the server. In both cases, the messages are not in temporary, intermediate storage, nor are they kept for any backup purpose.

Our interpretation also does not render irrelevant the more liberal access standards governing messages stored by remote computing services. *See* 18 U.S.C. §§ 2702(a)(2), 2703(b). The government's premise is that a message stored by a remote computing service "solely for the purpose of providing storage or computer processing services to [the] subscriber," *id.* §§ 2702(a)(2)(B), 2703(b)(2)(B), would also necessarily be stored for purposes of backup protection under section 2510(17)(B), and thus would be subject to the more stringent rules governing electronic storage. But not all remote computing services are also electronic communications services and, as to those that are not, section 2510(17)(B) is by its own terms inapplicable. The government notes that remote computing services and electronic communications services are "often the same entities," but "often" is not good enough to make the government's point. Even as to remote computing services that are also electronic communications services, not all storage covered by sections 2702(a)(2)(B) and 2703(b)(2)(B) is also covered by section 2510(17)(B). A remote computing service might be the only place a user stores his messages; in that case, the messages are not stored for backup purposes.

Finally, the government invokes legislative history. It cites a passage from a 1986 report indicating that a committee intended that messages stored by a remote computing service would "continue to be covered by section 2702(a)(2)" if left on the server after user access. H.R. Rep. No. 647, 99th Cong., at 65 (1986). The cited discussion addresses provisions relating to remote computing services. We do not read it to address whether the electronic storage provisions also apply. *See id.* at 64-65. The committee's statement that section 2702(a)(2) would "continue" to cover e-mail upon access supports our reading. If section 2702(a)(2) applies to e-mail even before access, the committee could not have been identifying an exclusive source of protection, since even the government concedes that unopened e-mail is protected by the electronic storage provisions.

The government also points to a subsequent, rejected amendment that would have made explicit the electronic storage definition's coverage of opened e-mail. *See* H.R. Rep. No. 932, 106th Cong., at 7 (2000). This sort of legislative history has very little probative value; Congress might have rejected the amendment precisely because it thought the definition already applied.

Finally, the government points to a passing reference in another recent report. H.R. Rep. No. 236(I), 107th Cong., at 57 (2001). The discussion addresses an unrelated issue and merely assumes that the definition only applies to unopened e-mail. This assumption was natural given that *Fraser* had recently been decided.

We acknowledge that our interpretation of the Act differs from the government's and do not lightly conclude that the government's reading is erroneous. Nonetheless, for the reasons above, we think that prior access is irrelevant to whether the messages at issue were in electronic storage. Because plaintiff's e-mail messages were in electronic storage regardless of whether they had been previously delivered, the district court's decision cannot be affirmed on this alternative ground.[4]

2. Plaintiffs also claim a violation of the Wiretap Act, which authorizes suit against those who "intentionally intercept[ ] . . . any wire, oral, or electronic communication."

---

[4] Defendants urge us to affirm on the additional ground that the complaint at one point alleges they "access[ed] . . . *Plaintiffs'* computer systems through which electronic communications systems are provided." Resp. Br. of Def./Appellee at 16 (emphasis added). Plaintiffs' computers, they note, are not "facilities" covered by 18 U.S.C. § 2701(a)(1), *Id.* at 15, We construe complaints liberally, however, *see Lynn v. Sheet Metal Workers' Int'l Ass'n*, 804 F.2d 1472, 1482 (9th Cir. 1986), and the substance of plaintiffs' claims is that defendants improperly accessed *NetGate's* servers.

18 U.S.C. §§ 2511(1)(a), 2520(a). We recently held in *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002), that the Act applies only to "acquisition contemporaneous with transmission." *Id.* at 878, Specifically, "'Congress did not intend for "intercept" to apply to "electronic communications" when those communications are in "electronic storage."'" *Id.* at 877 (quoting *Steve Jackson Games*, 36 F.3d at 462). *Konop* is dispositive, and the district court correctly dismissed the claim.

3. Plaintiffs finally claim a violation of the Computer Fraud and Abuse Act, which provides a cause of action against one who, inter alia, "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer if the conduct involved an interstate or foreign communication." 18 U.S.C. § 1030(a)(2)(C), (g). The conduct must involve one of five factors listed in 18 U.S.C. § 1030(a)(5)(B), which include a loss in excess of $5000. *Id.* § 1030(a)(5)(B)(i), (g).[5]

The district court dismissed without leave to amend on the theory that the Act does not apply to unauthorized access of a third party's computer. It also dismissed for failure to allege damages or loss, though it noted that this omission might be cured by amendment. Plaintiffs do not dispute the latter defect, but urge us to reverse as to the former ground so they can amend.

---

[5] Defendants argue that subsection (a)(5)(A) prescribes the Act's only civil offenses. But subsection (g) applies to any violation of "this section" and, while the offense must involve one of the five factors in (a)(5)(B), it need not be one of the three offenses in (a)(5)(A).

The district court erred by reading an ownership or control requirement into the Act. The civil remedy extends to *"[a]ny person* who suffers damage or loss by reason of a violation of this section." 18 U.S.C. § 1030(g) (emphasis added). " '[T]he word "any" has an expansive meaning, that is, "one or some indiscriminately of whatever kind."' " *HUD v. Rucker*, 535 U.S. 125, 131 (2002) (quoting *United States v. Gonzales*, 520 U.S. 1, 5 (1997)). Nothing in the provision's language supports the district court's restriction. Individuals other than the computer's owner may be proximately harmed by unauthorized access, particularly if they have rights to data stored on it.

Defendants argue in the alternative that NetGate authorized their access. Our earlier discussion disposes of this defense. They further contend that any damages or loss plaintiffs suffered do not fall within the Act's ambit. Because plaintiffs have not yet alleged the damages or loss they suffered, it would be premature to consider the argument.

4. Defendants contend they are immune from liability under the *Noerr-Pennington* doctrine, which exempts petitioning of public authorities from civil liability on First Amendment grounds. *See Manistee Town Ctr. v. City of Glendale*, 227 F.3d 1090, 1092 (9th Cir. 2000); *Kottle v. Northwest Kidney Ctrs.*, 146 F.3d 1056, 1059 (9th Cir. 1998). Lawsuits are protected by the doctrine because they are essentially petitions to the courts for redress of grievances. *See Cal. Motor Transp. Co. v. Trucking Unlimited*, 404 U.S. 508, 510 (1972). The doctrine is typically invoked to immunize the act of petitioning itself—i.e., the filing of the lawsuit. But it has been extended to certain conduct "incidental to the prosecution of the suit," for example, deciding whether to settle a claim. *See Columbia Pictures Indus., Inc. v. Prof'l Real Estate Investors, Inc.*, 944

F.2d 1525, 1528-29 (9th Cir. 1991), *aff'd,* 508 U.S. 49 (1993). Defendants seize on this language from *Columbia Pictures* and argue that, because the subpoena was incidental to their litigation, they are entitled to immunity.

We are skeptical that *Noerr-Pennington* applies at all to the type of conduct at issue. Subpoenaing private parties in connection with private commercial litigation bears little resemblance to the sort of governmental petitioning the doctrine is designed to protect. Nevertheless, assuming *arguendo* the defense is available, it fails. *Noerr-Pennington* does not protect "objectively baseless" sham litigation. *See Prof'l Real Estate Investors, Inc. v. Columbia Pictures Indus., Inc.*, 508 U.S. 49, 60 (1993). The magistrate judge found that the subpoena was "transparently and egregiously" overbroad and that defendants acted with gross negligence and in bad faith. This is tantamount to a finding that the subpoena was objectively baseless.

Defendants urge us to look only at the merits of the underlying litigation, not at the subpoena. They apparently think a litigant should have immunity for any and all discovery abuses so long as his lawsuit has some merit. Not surprisingly, they offer no authority for that implausible proposition. Assuming *Noerr-Pennington* applies at all, we hold that it is no bar where the challenged discovery conduct itself is objectively baseless.[6]

---

[6] *Noerr-Pennington's* sham litigation exception also requires proof of subjective intent to use legal process to achieve the evil prohibited by the statute from which exemption is claimed. *See Prof'l Real Estate Investors*, 508 U.S. at 60-61. That prong of the test is also satisfied here; presumably, the purpose of *any* objectively baseless subpoena is to uncover private information.

5. Having dismissed all the federal claims, the district court declined jurisdiction over the pendent state law claims under 28 U.S.C. § 1367(c)(3). Because we reverse dismissal of some of the federal claims, we "also reinstate the state claims.

We REVERSE dismissal of the Stored Communications Act claim, AFFIRM dismissal of the Wiretap Act claim, and REVERSE dismissal with prejudice of the Computer Fraud and Abuse Act claim with instructions to dismiss with leave to amend. We also REVERSE dismissal of the state claims.

AFFIRMED in part, REVERSED in part and remanded. Costs to appellants.

APPENDIX B

UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

No. 02-15742, No. 03-15301

[Filed August 28, 2003]

George Theofel; Howard Teig; David Kelley;)
Integrated Capital Associates, Inc., a Delaware)
Corporation; Nancy Rilett; Ryan Tam; Claudia)
English; Teresa Patterson; Tanya Young; Roberto)
Marsella; Regina Ovenden; Emil Pesiri; Eric)
Sullivan; Douglas H. Wolf; Richard Buckingham,)
Plaintiffs-Appellants,)
)
v.)
)
Alwyn Farey-Jones; Iryna A. Kwasny,)
Defendants-Appellees.)
--)
George Theofel; Howard Teig; David Kelley;)
Integrated Capital Associates, Inc., a Delaware)
Corporation; Nancy Rilett; Ryan Tam; Claudia)
English; Teresa Patterson; Tanya Young; Roberto)
Marsella; Regina Ovenden; Emil Pesiri; Eric)
Sullivan; Douglas H. Wolf; Richard Buckingham,)
Plaintiffs-Appellants,)
)
v.)

Alwyn Farey-Jones; Iryna A. Kwasny,)
Defendants-Appellees.)
_______________________________________)

Appeal from the United States District Court
for the Northern District of California
No. CV-01-04166-MMC

Maxine M. Chesney, District Judge, Presiding

Before: Betty B. Fletcher, Alex Kozinski and Stephen S. Trott, Circuit Judges.

OPINION

KOZINSKI, Circuit Judge:

We consider whether defendants violated federal electronic privacy and computer fraud statutes when they used a "patently unlawful" subpoena to gain access to e-mail stored by plaintiffs' Internet service provider.

Background

Plaintiffs Wolf and Buckingham, officers of Integrated Capital Associates, Inc. (ICA), are embroiled in commercial litigation in New York against defendant Farey-Jones. In the course of discovery, Farey-Jones sought access to ICA's e-mail. He told his lawyer Iryna Kwasny to subpoena ICA's ISP, NetGate.

Under the Federal Rules, Kwasny was supposed to "take reasonable steps to avoid imposing undue burden or expense" on NetGate. Fed. R. Civ. P. 45(c)(1). One might have thought, then, that the subpoena would request only e-mail related to the subject matter of the litigation, or maybe messages sent during some relevant time period, or at the very least those sent to or from employees in some way connected to the litigation. But Kwasny ordered production of "all copies of e-mails sent or received by anyone" at ICA, with no limitation as to time or scope.

NetGate, which apparently was not represented by counsel, explained that the amount of e-mail covered by the subpoena was substantial. But defendants did not relent. NetGate then took what might be described as the "Baskin-Robbins" approach to subpoena compliance and offered defendants a "free sample" consisting of 339 messages. It posted copies of the messages to a NetGate website where, without notifying opposing counsel, Kwasny and Farey-Jones read them. Most were unrelated to the litigation, and many were privileged or personal.

When Wolf and Buckingham found out what had happened, they asked the court to quash the subpoena and award sanctions. Magistrate Judge Wayne Brazil soundly roasted Farey-Jones and Kwasny for their conduct, finding that "the subpoena, on its face, was massively overbroad" and "patently unlawful," that it "transparently and egregiously" violated the Federal Rules, and that defendants "acted in bad faith" and showed "at least gross negligence in the crafting of the subpoena." He granted the motion to quash and socked defendants with over $9000 in sanctions to cover Wolf and Buckingham's legal fees. Defendants did not appeal that award.

Wolf, Buckingham and other ICA employees whose e-mail was included in the sample also filed this civil suit against Farey-Jones and Kwasny. They claim defendants violated the Stored Communications Act, 18 U.S.C. § 2701 *et seq.*, the Wiretap Act, 18 U.S.C. § 2511 *et seq.*, and the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, as well as various state laws. The district court held that none of the federal statutes applied, and dismissed the claims without leave to amend. It declined jurisdiction over the state law claims under 28 U.S.C. § 1367(c)(3). Plaintiffs now appeal.

Analysis

1. The Stored Communications Act provides a cause of action against anyone who "intentionally accesses without authorization a facility through which an electronic communication service is provided . . . and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage." 18 U.S.C. §§ 2701(a)(1), 2707(a). "[E]lectronic storage" means either "temporary, intermediate storage . . . incidental to . . . electronic transmission," or "storage . . . for purposes of backup protection." *Id.* § 2510(17). The Act exempts, inter alia, conduct "authorized . . . by the person or entity providing a wire or electronic communications service," *id.* § 2701(c)(1), or "by a user of that service with respect to a communication of or intended for that user," *id.* § 2701(c)(2).

The district court dismissed on the ground that NetGate had authorized defendants' access. It held that this consent was not coerced, because the subpoena itself informed NetGate of its right to object. Plaintiffs contend that NetGate's authorization was nonetheless invalid because the subpoena was patently unlawful. Their claim turns on the meaning of the word "authorized" in section 2701. We have previously reserved judgment on this question, *see Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 879 n.8 (9th Cir. 2002), while other circuits have considered related issues, *see, e.g.*, *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d

577, 582 n.10 (1st Cir. 2001) (holding access might be "unauthorized" under the Computer Fraud and Abuse Act if it is "not in line with the reasonable expectations" of the party granting permission (internal quotation marks omitted)); *United States v. Morris*, 928 F.2d 504, 510 (2d Cir. 1991) (holding access unauthorized where it is not "in any way related to [the system's] intended function").

We interpret federal statutes in light of the common law. *See Beck v. Prupis*, 529 U.S. 494, 500-01, 120 S. Ct. 1608, 146 L. Ed. 2d 561 (2000). Especially relevant here is the common law of trespass. Like the tort of trespass, the Stored Communications Act protects individuals' privacy and proprietary interests. The Act reflects Congress's judgment that users have a legitimate interest in the confidentiality of communications in electronic storage at a communications facility. Just as trespass protects those who rent space from a commercial storage facility to hold sensitive documents, *cf. Prosser and Keeton on the Law of Torts* § 13, at 78 (W. Page Keeton ed., 5th ed. 1984), the Act protects users whose electronic communications are in electronic storage with an ISP or other electronic communications facility.

A defendant is not liable for trespass if the plaintiff authorized his entry. *See Prosser & Keeton* § 13, at 70. But "an overt manifestation of assent or willingness would not be effective . . . if the defendant knew, or probably if he ought to have known in the exercise of reasonable care, that the plaintiff was mistaken as to the nature and quality of the invasion intended." *Id.* § 18, at 119; *cf. Restatement (Second) of Torts* §§ 173, 892B(2). Thus, the busybody who gets permission to come inside by posing as a meter reader is a trespasser. *J.H. Desnick, M.D., Eye Servs., Ltd. v. ABC*, 44 F.3d 1345, 1352 (7th Cir. 1995). So too is the police officer who, invited into a home, conceals a recording device for the

media. *Cf. Berger v. Hanlon*, 129 F.3d 505, 516-17 (9th Cir. 1997), *vacated*, 526 U.S. 808, 119 S. Ct. 1706, 143 L. Ed. 2d 978 (1999), *reinstated in relevant part*, 188 F.3d 1155, 1157 (9th Cir. 1999).

Not all deceit vitiates consent. "The mistake must extend to the essential character of the act itself, which is to say that which makes it harmful or offensive, rather than to some collateral matter which merely operates as an inducement." *Prosser & Keeton* § 18, at 120 (footnote omitted). In other words, it must be a "substantial mistake[ ] . . . concerning the nature of the invasion or the extent of the harm." *Restatement (Second) of Torts* § 892B(2) cmt. g. Unlike the phony meter reader, the restaurant critic who poses as an ordinary customer is not liable for trespass, *Desnick*, 44 F.3d at 1351; nor, unlike the wired cop, is the invitee who conceals only an intent to repeat what he hears, *cf. Dietemann v. Time, Inc.*, 449 F.2d 245, 249 (9th Cir. 1971)(invasion of privacy claim). These results hold even if admission would have been refused had all the facts been known.

These are fine and sometimes incoherent distinctions. *See Med. Lab. Mgmt. Consultants v. ABC*, 30 F. Supp. 2d 1182, 1201-04 (D. Ariz. 1998), *aff'd*, 306 F.3d 806 (9th Cir. 2002). But the theory is that some invited mistakes go to the essential nature of the invasion while others are merely collateral. Classification depends on the extent to which the intrusion trenches on "the specific interests that the tort of trespass seeks to protect." *Desnick*, 44 F.3d at 1352; *see also Lewis v. United States*, 385 U.S. 206, 211, 87 S. Ct. 424, 17 L. Ed. 2d 312 (1966); *Food Lion, Inc. v. Capital Cities/ABC, Inc.*, 194 F.3d 505, 517-18 (4th Cir. 1999).

We construe section 2701 in light of these doctrines. Permission to access a stored communication does not constitute valid authorization if it would not defeat a trespass claim in analogous circumstances. Section 2701(c)(1) therefore provides no refuge for a defendant who procures consent by exploiting a known mistake that relates to the essential nature of his access.

Under this standard, plaintiffs have alleged facts that vitiate NetGate's consent. NetGate disclosed the sample in response to defendants' purported subpoena. Unbeknownst to NetGate, that subpoena was invalid. This mistake went to the essential nature of the invasion of privacy. The subpoena's falsity transformed the access from a bona fide state-sanctioned inspection into private snooping. *See Restatement (Second) of Torts* § 174 (addressing "consent induced by fraud or mistake as to the validity of purported legal authority"); *cf. Bumper v. North Carolina*, 391 U.S. 543, 549, 88 S. Ct. 1788, 20 L. Ed. 2d 797 (1968) ("A search conducted in reliance upon a warrant cannot later be justified on the basis of consent if it turns out that the warrant was invalid."). The false subpoena caused disclosure of documents that otherwise would have remained private; it effected an "invasion . . . of the specific interests that the [statute] seeks to protect." *Desnick*, 44 F.3d at 1352.

Defendants had at least constructive knowledge of the subpoena's invalidity. It was not merely technically deficient, nor a borderline case over which reasonable legal minds might disagree. It "transparently and egregiously" violated the Federal Rules, and defendants acted in bad faith and with gross negligence in drafting and deploying it.[1] They are charged with knowledge of its invalidity. *See Prosser & Kee*ton § 18, at 119 (consent likely vitiated where defendants "ought to have known in the exercise of reasonable care" of the mistake).[2]

---

[1] Defendants had a full and fair opportunity to litigate the validity and good faith of the subpoena in the sanctions proceedings. Those proceedings were filed as a miscellaneous

That NetGate could have objected is immaterial. The subpoena may not have been coercive, but it was deceptive, and that is an independent ground for invalidating consent. *See Restatement (Second) of Torts* § 892B(2)-(3). It was a piece of paper masquerading as legal process. NetGate produced the sample in response and doubtless would not have done so had it known the subpoena was void -- particularly in light of its own legal obligation not to disclose such messages to third parties, *see* 18 U.S.C. § 2702(a)(1). That NetGate could have objected proves disclosure was not an inevitable consequence, but it was still a foreseeable one (and the intended one).

---

action on a separate docket from both the underlying New York litigation and the instant suit; defendants did not appeal. The magistrate's findings are therefore preclusive. *Cf.* 18 James Wm. Moore et al., *Moore's Federal Practice* § 132.03[4][k][vii], at 132-126 (3d ed. 1997) (judgment of contempt is issue preclusive); 3 Ronald E. Mallen & Jeffrey M. Smith, *Legal Malpractice* § 21.14, at 286 (5th ed. 2000) (attorney disciplinary proceedings may be issue preclusive).

[2] Prosser and Keeton say that constructive knowledge of a mistake is only "probably" sufficient to vitiate consent. *Prosser & Keeton* § 18, at 119. Whether or not ordinary negligence would suffice, the gross negligence and bad faith in this case are enough to charge defendants with constructive knowledge of the subpoena's invalidity.

Allowing consent procured by known mistake to serve as a defense would seriously impair the statute's operation. A hacker could use someone else's password to break into a mail server and then claim the server "authorized" his access. Congress surely did not intend to exempt such intrusions — indeed, they seem the paradigm of what it sought to prohibit. *Cf. Morris*, 928 F.2d at 510 (access gained by guessing someone else's password is not "authorization" under the Computer Fraud and Abuse Act).

The subpoena power is a substantial delegation of authority to private parties, and those who invoke it have a grave responsibility to ensure it is not abused. Informing the person served of his right to object is a good start, *see* Fed. R. Civ. P. 45(a)(1)(D), but it is no substitute for the exercise of independent judgment about the subpoena's reasonableness. Fighting a subpoena in court is not cheap, and many may be cowed into compliance with even overbroad subpoenas, especially if they are not represented by counsel or have no personal interest at stake. Because defendants procured consent by exploiting a mistake of which they had constructive knowledge, the district court erred by dismissing based on that consent.

Defendants ask us to affirm on the alternative ground that the messages they accessed were not in "electronic storage" and therefore fell outside the Stored Communications Act's coverage. *See* 18 U.S.C. § 2701(a)(1). The Act defines "electronic storage" as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." *Id.* § 2510(17), *incorporated by id.* § 2711(1). Several courts have held that subsection (A) covers e-mail messages stored on an ISP's server pending delivery to the recipient. *See In re Doubleclick, Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 511-12 (S.D.N.Y. 2001); *Fraser v. Nationwide Mut. Ins. Co.*, 135 F. Supp. 2d 623, 635-36 (E.D. Pa. 2001); *cf. Steve Jackson Games, Inc. v. U.S. Secret Serv.*, 36 F.3d 457, 461-62 (5th Cir. 1994)(messages stored on a BBS pending delivery). Because subsection (A) applies only to messages in "temporary, intermediate storage," however, these courts have limited that subsection's coverage to messages not yet delivered to their intended recipient. *See Doubleclick*, 154 F. Supp. 2d at 512; *Fraser*, 135 F. Supp. 2d at 636.

Defendants point to these cases and argue that messages remaining on an ISP's server after delivery no longer fall within the Act's coverage. But, even if such messages are not within the purview of subsection (A), they do fit comfortably within subsection (B). There is no dispute that messages remaining on NetGate's server after delivery are stored "by an electronic communication service" within the meaning of 18 U.S.C. § 2510(17)(B). *Cf. Doubleclick*, 154 F. Supp. 2d at 511 (holding that subsection (B) did not apply because the communications at issue were not being stored by an electronic communication service). The only issue, then, is whether the messages are stored "for purposes of backup protection." 18 U.S.C. § 2510(17)(B). We think that, within the ordinary meaning of those terms, they are.

An obvious purpose for storing a message on an ISP's server after delivery is to provide a second copy of the message in the event that the user needs to download it again — if, for example, the message is accidentally erased from the user's own computer. The ISP copy of the message functions as a "backup" for the user. Notably, nothing in the Act requires that the backup protection be for the benefit of the

ISP rather than the user. Storage under these circumstances thus literally falls within the statutory definition.[3]

One district court reached a contrary conclusion, holding that "backup protection" includes only temporary backup storage pending delivery, and not any form of "post-transmission storage." *See Fraser*, 135 F. Supp. 2d at 633-34, 636. We reject this view as contrary to the plain language of the Act. In contrast to subsection (A), subsection (B) does not distinguish between intermediate and post-transmission storage. Indeed, *Fraser's* interpretation renders subsection (B) essentially superfluous, since temporary backup storage pending transmission would already seem to qualify as "temporary, intermediate storage" within the meaning of subsection (A). By its plain terms, subsection (B) applies to backup storage regardless of whether it is intermediate or post-transmission.

Because plaintiffs' e-mail messages were in electronic storage regardless of whether they had been previously delivered, the district court's decision cannot be affirmed on this alternative ground.[4]

---

[3] That defendants did not read the messages until NetGate posted them to a website is immaterial. Defendants' unlawful subpoena caused NetGate to retrieve the messages from electronic storage and make them available. That constitutes "access" within the meaning of the Act.

[4] Defendants urge us to affirm on the additional ground that the complaint at one point alleges they "accessed . . . *Plaintiffs'* computer systems through which electronic communications systems are provided." Resp. Br. of Def./Appellee at 16 (emphasis added). Plaintiffs' computers, they note, are not "facilities" covered by 18 U.S.C. § 2701(a)(1). *Id.* at 15. We construe complaints

2. Plaintiffs also claim a violation of the Wiretap Act, which authorizes suit against those who "intentionally intercept[ ] . . . any wire, oral, or electronic communication." 18 U.S.C. §§ 2511(1)(a), 2520(a). We recently held in *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002), that the Act applies only to "acquisition contemporaneous with transmission." *Id.* at 878. Specifically, "'Congress did not intend for "intercept" to apply to "electronic communications" when those communications are in "electronic storage."'" *Id.* at 877 (quoting *Steve Jackson Games*, 36 F.3d at 462). *Konop* is dispositive, and the district court correctly dismissed the claim.

3. Plaintiffs finally claim a violation of the Computer Fraud and Abuse Act, which provides a cause of action against one who, inter alia, "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer if the conduct involved an interstate or foreign communication." 18 U.S.C. § 1030(a)(2)(C), (g). The conduct must involve one of five factors listed in 18 U.S.C. § 1030(a)(5)(B), which include a loss in excess of $5000. *Id.* § 1030(a)(5)(B)(i), (g).[5]

---

liberally, however, *see Lynn v. Sheet Metal Workers' Int'l Ass'n*, 804 F.2d 1472, 1482 (9th Cir. 1986), and the substance of plaintiffs' claims is that defendants improperly accessed *NetGate's* servers.

[5] Defendants argue that subsection (a)(5)(A) prescribes the Act's only civil offenses. But subsection (g) applies to any violation of "this section" and, while the offense must involve one of the five factors in (a)(5)(B), it need not be one of the three offenses in (a)(5)(A).

The district court dismissed without leave to amend on the theory that the Act does not apply to unauthorized access of a third party's computer. It also dismissed for failure to allege damages or loss, though it noted that this omission might be cured by amendment. Plaintiffs do not dispute the latter defect, but urge us to reverse as to the former ground so they can amend.

The district court erred by reading an ownership or control requirement into the Act. The civil remedy extends to "*[a]ny person* who suffers damage or loss by reason of a violation of this section. "18 U.S.C. § 1030(g) (emphasis added). "'[T]he word "any" has an expansive meaning, that is, "one or some indiscriminately of whatever kind.'" *HUD v. Rucker*, 535 U.S. 125, 131, 152 L. Ed. 2d 258, 122 S. Ct. 1230 (2002) (quoting *United States v. Gonzales*, 520 U.S. 1, 5, 137 L. Ed. 2d 132, 117 S. Ct. 1032 (1997)). Nothing in the provision's language supports the district court's restriction. Individuals other than the computer's owner may be proximately harmed by unauthorized access, particularly if they have rights to data stored on it.

Defendants argue in the alternative that NetGate authorized their access. Our earlier discussion disposes of this defense. They further contend that any damages or loss plaintiffs suffered do not fall within the Act's ambit. Because plaintiffs have not yet alleged the damages or loss they suffered, it would be premature to consider the argument.

4. Defendants contend they are immune from liability under the *Noerr-Pennington* doctrine, which exempts petitioning of public authorities from civil liability on First Amendment grounds. *See Manistee Town Ctr. v. City of Glendale*, 227 F.3d 1090, 1092 (9th Cir. 2000); *Kottle v. Northwest Kidney Ctrs.*, 146 F.3d 1056, 1059 (9th Cir.

1998). Lawsuits are protected by the doctrine because they are essentially petitions to the courts for redress of grievances. *See Cal. Motor Transp. Co. v. Trucking Unlimited*, 404 U.S. 508, 510, 30 L. Ed. 2d 642, 92 S. Ct. 609 (1972). The doctrine is typically invoked to immunize the act of petitioning itself — i.e., the filing of the lawsuit. But it has been extended to certain conduct "incidental to the prosecution of the suit," for example, deciding whether to settle a claim. *See Columbia Pictures Indus., Inc. v. Prof'l Real Estate Investors, Inc.*, 944 F.2d 1525, 1528-29 (9th Cir. 1991), *aff'd*, 508 U.S. 49, 123 L. Ed. 2d 611, 113 S. Ct. 1920 (1993). Defendants seize on this language from *Columbia Pictures* and argue that, because the subpoena was incidental to their litigation, they are entitled to immunity.

We are skeptical that *Noerr-Pennington* applies at all to the type of conduct at issue. Subpoenaing private parties in connection with private commercial litigation bears little resemblance to the sort of governmental petitioning the doctrine is designed to protect. Nevertheless, assuming *arguendo* the defense is available, it fails. *Noerr-Pennington* does not protect "objectively baseless" sham litigation. *See Prof'l Real Estate Investors, Inc. v. Columbia Pictures Indus., Inc.*, 508 U.S. 49, 60, 113 S. Ct. 1920, 123 L. Ed. 2d 611 (1993). The magistrate judge found that the subpoena was "transparently and egregiously" overbroad and that defendants acted with gross negligence and in bad faith. This is tantamount to a finding that the subpoena was objectively baseless.

Defendants urge us to look only at the merits of the underlying litigation, not at the subpoena. They apparently think a litigant should have immunity for any and all discovery abuses so long as his lawsuit has some merit. Not surprisingly, they offer no authority for that implausible proposition. Assuming *Noerr-Pennington* applies at all, we hold that it is no bar where the challenged discovery conduct itself is objectively baseless.[6]

5. Having dismissed all the federal claims, the district court declined jurisdiction over the pendent state law claims under 28 U.S.C. § 1367(c)(3). Because we reverse dismissal of some of the federal claims, we also reinstate the state claims.

We REVERSE dismissal of the Stored Communications Act claim, AFFIRM dismissal of the Wiretap Act claim, and REVERSE dismissal with prejudice of the Computer Fraud and Abuse Act claim with instructions to dismiss with leave to amend. We also REVERSE dismissal of the state claims.

AFFIRMED in part, REVERSED in part and remanded. Costs to appellants.

---

[6] *Noerr-Pennington*'s sham litigation exception also requires proof of subjective intent to use legal process to achieve the evil prohibited by the statute from which exemption is claimed. *See Prof'l Real Estate Investors*, 508 U.S. at 60-61. That prong of the test is also satisfied here; presumably, the purpose of *any* objectively baseless subpoena is to uncover private information.

APPENDIX C

IN THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA

Case No. 01-4166 MMC

(Docket No. 9)

[Filed March 8, 2002]

GEORGE THEOFEL, et. al.,
Plaintiffs,

v.

ALWYN FAREY-JONES, an individual,
IRYNA A. KWASNY, an individual.
Defendants.

ORDER GRANTING MOTION TO DISMISS

Before the Court is defendant Alwyn V.H. Farey-Jones' ("Farey-Jones") motion to dismiss, filed December 21, 2001, pursuant to Rule 12(b)(6) of the Federal Rules of Civil Procedure.[1] Plaintiffs have filed opposition, to which defendant replied. Having considered the papers filed in support of and in opposition to the motion, the Court deems the motion appropriate for decision on the papers, hereby VACATES the hearing scheduled for March 1,2002, and rules as follows:

---

[1] On January 11,2002, Farey-Jones filed a motion for Rule 11 sanctions. On February 15, 2002, Farey-Jones withdrew the motion pursuant to Civil Local Rule 7-7(e), which allows the moving party

BACKGROUND

This case arises out of a subpoena served by defendant Farey-Jones and his counsel, defendant Iryna A. Kwasny ("Kwasny"), in connection with an action entitled Farey-Jones v. Buckingham, et. al., (Case No. CV 99 4205, E.D.N.Y.) ("Farey-Jones action"). On September 25, 2001, defendants served the subpoena on NetGate Internet ("NetGate"), an Internet service provider, seeking electronic and other documents maintained by NetGate. NetGate provides email services to plaintiff Integrated Capital Associates, Inc. ("ICA") as well as its employees, staff, and "related and affiliated entities and individuals," including the individual plaintiffs in this action. (See Compl. ¶¶ 30, 31.) On February 1, 2002, Magistrate Judge Wayne D. Brazil quashed the subpoena, finding that the subpoena was "grossly overbroad" and that the communications sought were likely to contain information that was "obviously irrelevant, and/or sensitive commercially (trade secrets) or personally, and/or privileged." (See Order Granting Motions to Quash and Sanctions, filed February 1,2002, at 1,4.) Magistrate Judge Brazil further concluded that defendants acted in bad faith in

---

to withdraw a motion within 7 days after service of opposition. Here, plaintiffs' opposition was filed February 8, 2002. Accordingly, Farey-Jones' notice of withdrawal was timely. Although plaintiffs object to withdrawal without prejudice, plaintiffs cite no authority, in support of their objection.

serving an overbroad subpoena, and in failing to provide prior notice to opposing counsel. (See id. at 6.)

On October 2, 2001, before the subpoena was quashed, NetGate uploaded a "sampling" of the subject electronic communications onto its website and provided defendants with a URL allowing defendants to access the sample. This sample contained over 300 emails, including attachments, that were stored on the NetGate server on August 14, 2001. (See Compl. ¶ 39.)

Plaintiffs allege that defendants violated plaintiffs' rights by requesting, receiving and copying the confidential and private emails provided by NetGate. Specifically, plaintiffs' allege seven claims for relief based on defendants' conduct: (1) Violation of the Electronic Communications Privacy Act - Stored Electronic Communications; (2) Violation of the Electronic Communications Privacy Act- Interception of Electronic Communications; (3) Violation of the Computer Fraud and Abuse Act; (4) Violation of California Constitution, Article I, Section 1 - Violation of State Constitutional Right of Privacy; (5) Violation of California Civil Code § 3426, et. seq.- California Trade Secrets Act; (6) Violation of Business and Professions Code § 17200 et. seq.; and (7) Conversion.

LEGAL STANDARD

A motion to dismiss under Rule 12(b)(6) cannot be granted unless "it appears beyond doubt that the plaintiff can prove no set of facts in support of his claim which would entitle him to relief." Conley v. Gibson, 355 U.S. 41,45-46 (1957). Dismissal can be based on the lack of a cognizable legal theory or the absence of sufficient facts alleged under a cognizable legal theory. See Balistreri v. Pacifica Police

Dept., 901 F.2d 696, 699 (9th Cir.1988). Dismissal is disfavored, however, and should be granted only in "extraordinary" cases. See United States v. Redwood City, 640 F.2d 963, 966 (9th Cir.1981).

Generally, a district court may not consider any material beyond the pleadings in ruling on a Rule 12(b)(6) motion. See Hal Roach Studios, Inc. v. Richard Feiner & Co., Inc., 896 F.2d 1542, 1555 n.19 (9th Cir.1989). Material which is properly submitted as part of the complaint may, however, be considered. See id. In addition, documents specifically referred to in a complaint, though not physically attached to the pleading, may be considered where authenticity is unquestioned. See Branch v. Tunnell, 14 F.3d 449;454 (9th Cir. 1994).

In analyzing a motion to dismiss, the Court must accept as true all material allegations in the complaint and construe them in the light most favorable to the nonmoving party. See NL Industries, Inc. v. Kaplan, 792 F.2d 896, 898 (9th Cir.1986). Facual allegations may be disregarded, however, if contradicted by documents to which the court may properly refer. See Durning v. First Boston Corp., 815 F.2d 1265, 1267 (9th Cir.1987). Conclusory allegations, unsupported by the facts alleged, need not be accepted as true. See Holden v. Hagopian, 978F.2d 1115, 1121 (9th Cir.1992).

DISCUSSION

A. Electronic Communications Privacy Act/ Stored Electronic Communications Act

In their first claim for relief, plaintiffs plead a violation of Title II of the Electronic Communications Privacy Act

("ECPA"), also known as the Stored Communications Act, 18 U.S.C. § 2701 et seq.[2]

1. Unauthorized Access

As explained by the Fifth Circuit, "Title II [of the ECPA] generally proscribes unauthorized access to stored wire or electronic communications." See Steve Jackson Games, Inc. v. United States Secret Service, 36 F. 3d 457,462 (5th Cir. 1994). Section 2701 (a) provides that Title II of the ECPA is violated by a person who

> (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
> (2) intentionally exceeds an authorization to access that facility and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system . . . .

See 18 U.S.C. § 2701(a). Section 2707(a) provides a civil cause of action for knowing or intentional violations of § 2701. See 18 U.S.C. § 2707(a).

Section 2701(c) provides for exceptions to liability created by § 2701(a) where the access is authorized by the person or entity providing the electronic communications-service. Specifically, §2701(c) states in relevant part:

---

[2] The Ninth Circuit has referred to 18 U.S.C. §§ 2761-2710 as the Stored Communications Act. See United States v. Smith, 155 F. 3d 1051, 1055 (9th Cir. 1998).

> Subsection (a) of [§ 2701] does not apply with respect to conduct authorized --
>
> (1) by the person or entity providing a wire or electronic communications service;
>
> (2) by a user of that service with respect to a communication of or intended for that user. . . .

See 18 U.S.C. § 2701(c).

Here, plaintiffs allege that defendants intentionally accessed plaintiffs' computers, without plaintiff's authorization or exceeding authorization, and thereby "obtained access to [p]laintiff's wire and electronic communications while in electronic storage in such computer systems."[3] (See id. ¶¶ 26, 49.) Although plaintiffs allege that defendants' access was without plaintiffs' consent, plaintiffs acknowledge that NetGate, plaintiffs' Internet service provider, "made [the confidential emails] available" to defendants. (See Compl. ¶¶ 27, 39.) As the facts pled in plaintiffs' complaint demonstrate that defendants' access was authorized by NetGate, plaintiffs have failed to state a claim based on unauthorized access.[4] See 18 U.S.C. § 2701(c).

---

[3] Plaintiffs allege their computers are "facilities" through which an "electronic communication service" is provided to them. (See Compl. at ¶ 49.) Farey-Jones argues that "facility" cannot refer to a personal computer. In light of the Court's dismissal of plaintiffs' Stored Communications Act claim on other grounds, see infra, the Court need not reach this issue.

[4] Although plaintiffs argue that NetGate was "coerced" by defendants' subpoena into supplying the information in question, plaintiffs provide no authority for this assertion. (See Opp'n at 14-15.) Rather, plaintiffs suggest that a subpoena is the equivalent of "putting a gun to [NetGate's] head." Hardly. See, e.g., Fed. R.

2. Disclosure

The Stored Communications Act also prohibits "a person or entity providing an electronic communication service" from "knowingly divulg[ing] to any person or entity the contents of a communication while in electronic storage by that service." See 18 U.S.C. § 2702 (a)(1).

Here, plaintiffs allege that defendants "knowingly divulged the contents of [plaintiff's wire and electronic] communications while in electronic storage." (See id. ¶ 49.) Plaintiffs, however, do not allege that Farey-Jones is "a person or entity providing an electronic communication service." To the contrary, plaintiffs' allege that NetGate provides plaintiffs' electronic communication services. (See Compl. ¶ 27.) As a result, plaintiffs cannot state a claim against Farey-Jones based on unauthorized disclosure.

Accordingly, plaintiffs' First Claim for Relief (Violation of the Electronic Communications Privacy Act - Stored Electronic Communications) is hereby DISMISSED.

B. Electronic Communications Privacy Act- Interception of Electronic Communications

In plaintiffs' second claim for relief, plaintiffs allege a violation of Title II of the Electronic Communications Privacy

---

Civ. Proc. 45(c)(2)(B). Indeed, the subpoena in question specifically informs the recipient of its right to move to quash on a variety of grounds, including privilege, undue burden and disclosure of trade secrets. (See Req. for Jud'l Notice Ex. A ¶¶ 3(A), (B).)

Act, which Act amended the Wiretap Act, 18 U.S.C. § 2510 et seq.

18 U.S.C. § 2511 (1)(a) provides for criminal penalties where a person "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication," see 18 U.S.C. § 2511 (1)(a), as well as where one person "intentionally discloses" to another, or "intentionally uses" the contents of any electronic communication "knowing or having reason to know that the information was obtained through the interception of [an]. . . electronic communication" in violation of the Wiretap Act. See 18 U.S.C. §§ 2511(1)(c) (disclosure), 2511(1)(d)(use). Section 2520(a) provides that "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity which engaged in that violation." See 18 U.S.C. § 2520(a).

Plaintiffs allege that "[d]efendants either directly or by aiding and abetting and/or conspiring to do so, intentionally intercepted, endeavored to intercept, used and/or disclosed Plaintiffs' electronic communications, . . . without Plaintiffs' knowledge, authorization or consent." (See Compl. ¶ 52.) Specifically, plaintiffs allege that defendants intercepted "email data on the NetGate server on August 14, 2001 ." (See Compl. ¶ 39.)

It is undisputed that the email messages in question were stored on NetGate's server and were nearly two months old at the time they were produced. Farey-Jones asserts that the subject email messages could not have been "intercepted" by defendants within the meaning of the Wiretap Act, as those messages were not acquired while "in transit" but rather were acquired after they had been stored. The Court agrees. Under the Wiretap Act, electronic communications can only be "intercepted" at the time the messages are being transmitted, not after they have been stored. See United States v. Smith, 155F.3d 1051, 1057 (1998)(holding "non-contemporaneous retrievals" of electronic communications are excepted from the scope of the Wiretap Act); United States v. Turk, 526 F.2d 654 (5th Cir. 1976)(holding interception "require[s] participation by the one charged with an 'interception' in the contemporaneous acquisition of the communication"); Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457,461-62 (5th Cir. 1994)(holding that "Congress did not intend for 'intercept' to apply to 'electronic communications' when those communications are in 'electronic storage.'")

Accordingly, plaintiffs' Second Claim for Relief (Violation of the Electronic Communications Privacy Act-Interception of Electronic Communications) is hereby DISMISSED.

C. Computer Fraud and Abuse Act

In plaintiffs third claim for relief, plaintiffs allege a violation of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030.[5] Pursuant to §1030(a)(5)(A), a person violates the CFAA when that person "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;" or "intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage;" or "intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage." See 18 U.S.C. § 1030(5)(A)(i),(ii),(iii). Here, plaintiffs allege that "Defendants knowingly accessed, without authorization and/or exceeding authorized access, Plaintiff's personal computers and obtained valuable-information from those computer systems in conjunction therewith." (See Compl. ¶ 55.)

---

[5] Farey-Jones argues, for the first time in his reply, that plaintiffs' CFAA claim and "all other non-constitutional Federal and State claims" must be dismissed because the ECPA provides the exclusive remedy for conduct regulated by the ECPA. In a letter sent to the Court, plaintiffs object to the inclusion in the reply of this new argument, as well as to Farey-Jones' citation of an unpublished opinion in support thereof. Plaintiffs request the opportunity to file a surreply. As the Court did not rely on the new argument in reaching its conclusions, plaintiffs request for leave to

1. Access to Plaintiffs' Computers

Farey-Jones argues that he did not "access" plaintiffs' computers within the meaning of the CFAA.[6]

Plaintiffs plead that defendants "accessed" plaintiffs' emails after NetGate electronically uploaded the emails to the NetGate website and provided Kwasny with the URL necessary to view the information. (See Compl. ¶ 39.) Although plaintiffs allege that defendants "accessed" plaintiff's computers to receive the emails in question, this conclusory statement is inconsistent with the facts as pleaded. (See Compl. ¶¶ 39, 55.) Plaintiffs argument that "NetGate

---

file a surreply is hereby DENIED.

[6] As noted, plaintiffs have not alleged that defendants transmitted a program or other information to plaintiffs' computers. Rather, plaintiffs reply on unauthorized access.

operates as an off site extension of plaintiffs' computers for the purposes of receiving, storing, and retransmitting plaintiffs' confidential emails" and that "defendants in effect accessed plaintiffs' own computers" by accessing plaintiffs' emails through NetGate is unavailing. (See Opp'n at 19). Plaintiffs cite no authority for the proposition that one can "in effect" access a computer within the meaning of the CFAA by accessing a third party's computer. Such an interpretation is inconsistent with the plain meaning of the § 1030(a)(5)(A)(ii) and (iii) of the CFAA. See 18 U.S.C. § 1030(5)(A)(ii) & (iii).

2. Damages

Under § 1030(g), plaintiffs are entitled to bring a civil action for violation of the CFAA if the conduct alleged "involves 1 of the factors set forth in clause (i), (ii), or (iii), (iv), or (v) of subsection (a)(5)(B).[7] See 18 U.S.C. § 1030(g). Under §1030(a)(5)(B)(i), the conduct must cause "loss to 1 or more persons during any 1 year period . . . aggregating at least $5,000 in value." See 18 U.S.C. § 1030(a)(5)(B)(i). "Loss" is defined as "any reasonable cost to any victim; including the cost of responding to an offense, conducting a damage assessment, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11).

Here, as Farey-Jones points out, there is no allegation in the complaint that plaintiffs suffered a "loss . . . during any 1 year period . . . aggregating at least $5,000 in value." See 18 U.S.C. § 1030(a)(5)(B)(i). To the contrary, plaintiffs' complaint is silent as to the specific amount of damages sustained. Consequently, plaintiffs' have failed to state a claim under the CFAA.

---

[7] It is undisputed that only §1030(a)(5)(B)(i)is applicable in the instant action.

Plaintiffs ordinarily would be afforded leave to amend to cure this deficiency. Here, however, even if plaintiffs' could amend to specify the requisite damages, such amendment would be futile as the facts alleged in plaintiffs' complaint demonstrate that defendants did not access plaintiffs' computers in violation of the CFAA.

Accordingly, plaintiff's Third Claim for Relief (Violation of the Computer Fraud and Abuse Act) is hereby DISMISSED.

C.State Law Causes of Action

As noted, plaintiff also pleads four state law causes of action: (1) Violation of California Constitution, Article I, Section 1 - Violation of State Constitutional Right of Privacy; (2) Violation of California Civil Code § 3426, et. seq. - California Trade Secrets Act; (3) Violation of Business and Professions Code § 17200 et. seq.; and (4) Conversion.

Farey-Jones argues that, if the Court dismisses plaintiffs' federal Claims, the Court should decline to exercise supplemental jurisdiction over plaintiff's state law claims. The Court agrees. See 28 U.S.C. § 1367(c)(3)(providing district court may decline to exercise supplemental jurisdiction over state claims when it has dismissed claims over which it has original jurisdiction).

Accordingly, in light of the Court's dismissal of plaintiff's federal claims, plaintiffs' state law claims are hereby DISMISSED without prejudice pursuant to 18 U.S.C. § 1367(c)(3).

CONCLUSION

For the reasons stated above, Farey-Jones' motion to dismiss is hereby GRANTED and plaintiffs' complaint is hereby DISMISSED.

This order closes Docket No. 9.

IT IS SO ORDERED.

Dated March 8, 2002

/s/ Maxine M. Chesney
United States District Judge

UNITED STATES DISTRICT COURT
FOR THE
NORTHERN DISTRICT OF CALIFORNIA

Case Number: C-01-4166 MMC

Certificate of Service

George Theofel, et al.,)
Plaintiff,)
)
v.)
)
Alwyn Farey-Jones and Iryna A. Kwasny,)
Defendant.)
)

I, the undersigned, hereby certify that I am an employee in the Office of the Clerk, U.S. District Court, Northern District of California.

That on March 8, 2002, I SERVED a true and correct copy(ies) of the attached, by placingsaid copy(ies) in a postage paid envelope addressed to the person(s) hereinafter listed, by depositing said envelope m the U.S. Mail, or by placing said copy(ies) into an inter-office delivery receptacle located in the Clerk's office.

Richard J. Idell
Owen Seitel
Jennifer Marone
Idell Berman & Seitel
530 Bush Street, Suite 601
San Francisco, CA 94108

Nicole A. Wong
Manuella W. Hancock
Perkins Coie
180 Townsend Street, 3rd Floor
San Francisco, CA 94107-1909

Dated: March 8, 2002

Richard W. Wieking, Clerk

/s/
Deputy Clerk

APPENDIX D

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

Case No. 01-0181 Misc. MMC (WDB)

[Filed February 1, 2002]

IN RE THE MATTER OF
THE SUBPOENA SERVED
ON NETGATE INTERNET

ALWYN V.H. FAREY-JONES,
Plaintiff(s),

v.

RICHARD G. BUCKINGHAM, et al.,
Defendant(s).

ORDER GRANTING MOTIONS TO QUASH AND SANCTIONS

On January 30, 2002, the court conducted a hearing in connection with defendants' Motion to Quash and Motion for Sanctions. For reasons set forth at length on the record during the hearing, the court enters the following Orders:

1. The defendants' Motion to Quash the subpoena to NetGate is **GRANTED**. The subpoena is grossly overbroad

and counsel's efforts to justify it (or some unclearly delineated modified version of it) fell far short of satisfying the requirements of Federal Rules of Civil Procedure 45, 26(b), and 26(g).

2. If plaintiff in the New York action elects to pursue discoverable information through NetGate by serving a second subpoena, he must craft a proposed new subpoena that is dramatically narrower in scope and specifically tailored to the matters in dispute in the pending litigation. Before serving NetGate, he must submit a copy of the proposed subpoena, accompanied by a proposed protective order, simultaneously to the undersigned and to counsel for defendants. Plaintiff also must accompany the proposed new subpoena with evidence and argument that demonstrate compliance with the relevance and proportionality requirements of the Federal Rules of Civil Procedure.

The court will permit the subpoena to issue only if it is satisfied, after giving defendants an opportunity to be heard, that issuance conforms to all the pertinent requirements of Federal Rules of Civil Procedure 45, 26(b), and 26(g).

Unless plaintiff makes a clear showing that the information sought in the revised subpoena is likely to contribute meaningfully to the truth finding process, that the information sought is not available from alternative sources, and that the burdens the subpoena will impose meet the applicable proportionality requirements, the court will require plaintiff not only to reimburse NetGate for all the expenses it reasonably incurs in responding, but also to pay the reasonable expenses (including attorneys fees) that defendants incur in connection with the processes that the subpoena triggers.

3. The record developed by the papers and at the hearing clearly supports a conclusion that defendants are entitled under the law to a fee shifting sanction. Considerations that support that conclusion include the following:

a. The subpoena as drafted and served by Ms. Kwasny (without limitations as to time, to subject matter, or to the persons or entities who sent or received emails) violated, transparently and egregiously, Federal Rule of Civil Procedure 45(c)(1), which requires "an attorney responsible for the issuance and service of a subpoena [to] take reasonable steps to avoid imposing undue burden or expense on a person subject to that subpoena." Neither Ms. Kwasny nor anyone else representing plaintiff took such steps - before or after (as will be explained below) she issued the subpoena. Nor did Ms. Kwasny offer anything approaching a substantial justification for this failure- she essentially admitted that she issued the subpoena without substantial guidance from plaintiff's counsel in New York about the nature of the matters in issue there, without knowing pertinent circumstances, and without seeking information from either defense counsel or NetGate. The subpoena was so broadly cast, she says, in part because her client knew so little about NetGate and its function and in part because plaintiff feared that any less sweeping demand would permit NetGate (a non-party) somehow to avoid disclosing important evidence. These are wholly inadequate excuses for failing to make the simple inquiries that would have resulted in informed, responsible, professional judgment about whether to issue the subpoena at all and, if so, how to tailor it to comply with the law.

The second sentence of Federal Rule of Civil Procedure 45(c)(1) requires the court that issued a subpoena to enforce the duty that is imposed in the first sentence of the Rule "and [to] impose upon the party or attorney in breach of this duty an appropriate sanction, which may include, but is not limited to, lost earnings and a reasonable attorney's fee." While this provision was intended primarily to protect non-party targets of subpoenas, courts could not meet their responsibility to enforce this Rule if they could not, in appropriate circumstances, award as a sanction fees and costs that a clear violation of this Rule caused a party to the litigation to suffer.

It appears that the issuance of this subpoena, as so broadly and thoughtlessly crafted, also violated Federal Rule of Civil Procedure 26(g), which requires a lawyer to certify, for every discovery request she makes, that "to the best of [her] knowledge, information, and belief, formed after a reasonable inquiry, the request . . . is (A) consistent with these rules . . . and (C) not unreasonable or unduly burdensome or expensive, given the needs of the case, the discovery already had in the case, the amouut in controversy, and the importance of the issues at stake in the litigation."

Neither Ms. Kwasny nor any other lawyer acting on plaintiff's behalf made the "reasonable inquiry" required by Rule 26(g) before the patently overbroad subpoena was drafted. And, as served, this subpoena obviously was unreasonable -- it failed to set forth any limit at all on either the subject matters it would reach or the time period it would cover. Courts also are required to impose sanctions for a violation of Rule 26(g)- absent a showing that the violation was substantially justified. No such showing has been made here. The sanctions contemplated contemplated expressly by Rule 26(g) "may include an order to pay the amount of the reasonable expenses incurred because of the violation, including a reasonable attorney's fee."

b. Neither Ms. Kwasny nor anyone else gave defendants (through counsel or otherwise "[p]rior notice of any commanded production of documents" as required by Rule 45(b)(1). Some courts have held that the "prior notice" required by this Rule means before the subpoena is issued. See, e.g., Biocore Medical Technologies v. Khosrowshahi, 181 F.R.D. 660, 667 (D. Kansas, 1998) (discussing the rule-background against which the current version of the rule was adopted), and Schweizer v. Mulvehill, 93 F.Supp.2d 376, 411 (S.D. NY 2000). At a minimum prior notice must mean notice that is essentially contemporaneous with the issuance of the subpoena – as later notice would jeopardize the primary purpose of the notice requirement – which is, as the Advisory Committee Note (1991) makes clear, "to afford other parties an opportunity to object to the production or inspection . . . (Emphasis added).

Ms. Kwasny, apparently as requested either by plaintiff himself or by plaintiff's counsel in New York, Mr. Metli, issued the subpoena on September 25, 2001. It was not until October 2, 2001, that a copy of the subpoena was given to defense counsel. That week delay, while by itself not a matter of great consequence in the specific circumstances here (the deadline for compliance by NetGate was October 29, 2001), was not justified.

c. On October 2, 2001, an employee of NetGate contacted Ms. Kwasny, informed her that the material sought in the subpoena was substantial, and suggested that he send her a URL that she could use to access a sample of the material that would fall within the scope of the subpoena. Even though Ms. Kwasny knew (or clearly should have known) that the plaintiffand the defendants were competitors, and that the emails might well include information that was obviously irrelevant, and/or sensitive commercially (trade secrets) or personally, and/or privileged, she sent the URL to plaintiff, who used it to access and download the sample production – a production that included well over 300 emails (many with substantial attachments, most not involving any party to the New York action). Most unprofessionally, Ms. Kwasny did not notify defendants that this sample production had been proposed or was completed. By failing to notify defense counsel before she agreed to the sample production, she clearly and foreseeably defeated the purposes of the notice requirement in Rule 45(b)(1) and facilitated an invasion of interests that could not be justified.

It was not until at least October 18, 2001, that defense counsel had any idea that the sample production had occurred and that plaintiff had had access, for more than two weeks, to communications that belonged to defendants. No justification at all has been advanced for the failure to notify defense counsel of the proposal by NetGate, for plaintiff's retrieval of the material without notice to defendants (in fact, plaintiff acquired the material on the same day that defense counsel first learned that the subpoena had issued), and for not disclosing any of this to defense counsel until more than two weeks after the fact.

d. Between October 17 and October 23, 2001, counsel for defendants and counsel for plaintiff conferred about the scope of the subpoena and the deadline for compliance. The record supports a finding that counsel for the parties would have been able to reach an agreement at least to extend the deadline for compliance (so the negotiations about scope could continue) but for the fact that plaintiff refused to extend the deadline unless defendants agreed "to refrain from accessing data from NetGate pending resolution of the scope of the Subpoena." Farey-Jones Declaration, January 8, 2002.

As his attorneys now concede, there was no legal basis for such a demand. The emails in issue belonged to the defendants – they were communications by or to the defendants and their colleagues that were merely being stored by NetGate. Moreover, the vast majority of the emails in question were quite recent – dating from August 15, 2001, through the date of the failed negotiations (October 23, 2001). It would have occurred to a reasonable person that defendants might well need to have access to some of these recent emails just to carry on their business.

As Ms. Kwasny reports, when defendants refused to accept this condition, plaintiff instructed her to inform counsel for defendants that plaintiff would not agree even to extend the October 29, 2001, deadline for the production under the subpoena.

On Wednesday, October 24, 2001, Ms. Kwasny left a voicemail message for defense counsel that included the following: "I just spoke with Alwyn Jones and Richard Metli and we don't see any way that we can narrow the scope of the subpoena at this point so we're not going to agree to either narrowing the scope of the subpoena or define the issues or extend the due date. I have to let you know that I'll be out of town beginning tomorrow and through the weekend so I guess you can send me [sic] by mail and I'Il review the papers when I return."

To repeat, the subpoena, on its face, was massively overbroad. Why plaintiff and his counsel could see no way to narrow its scope is dumfounding. Nor have they offered anything approaching an adequate justification for terminating the meet and confer process and for refusing to extend the deadline for what would obviously be an overbroad and unjustifiable production.

Defense counsel had warned plaintiff's attorneys, in writing on October 17th, and again orally on October 23/24, that their refusal to extend the deadline for return on the subpoena past Monday, October 29th, would leave him with no choice but to seek file a motion to quash and to seek an emergency order shortening time. When Ms. Kwasny, on orders from her client, refused to budge (then left town, making herself unavailable during the last few days before the return date), defense counsel was forced to file papers that he never would have been forced to file if plaintiff and his counsel had not insisted on imposing an obviously unreasonable and legally unsupportable condition.

The course of conduct just described supports a finding, which the court hereby makes, that plaintiff and his counsel acted in bad faith in these matters. There was at least gross negligence in the crafting of the subpoena; there was bad faith in not disclosing the proposed (then executed) sample production; and there was bad faith in terminating the meet and confer process when defendants would not agree to the unjustifiable condition on which plaintiff insisted. By this course of conduct, plaintiff and his counsel, without justification, forced defendants to incur substantial legal fees (among other burdens). It is patently unfair to make defendants bear the economic burden caused by such unprofessional and unjustified conduct. And there is no question that legitimate concerns necessitated the protective actions that defense counsel were so unreasonably forced to take: the huge number of e-mails potentially subject to the subpoena (many of very recent origin) likely contained material that was sensitive, protected by law from disclosure, and irrelevant. The e-mails also included large numbers of presumptively private communications made by or to persons who had nothing to do with the case.

The record further supports a finding that the plaintiff, Ms. Kwasny, and Mr. Metli (lead counsel for plaintiff in the New York action – and therefore responsible, ultimately, for guiding local counsel here in California) all share substantial responsibility for this course of conduct – and therefore that each of these three persons is liable for one-third of the monetary sanction hereby imposed.

On this record, sanctions are authorized (indeed, compelled) by Federal Rules of Civil Procedure 26(c) and (g), 37(a)(4), and 45(c)(1), as well as under the court's inherent authority.

Declarations submitted by Mr. Idell and Ms. Marone, local counsel for defendants, and the many papers they have filed in this matter, serve as sufficient sources of evidence to inform a reasonable judgment by this court about the amount of time competent lawyers would have been required to spend (over the period infected by the unjustifiable conduct by plaintiff and his counsel in connection with this subpoena) to protect their clients and others from the unwarranted burdens and invasions of interests that a production of the emails covered by the subpoena would have caused. **It is this court's judgment that counsel for defendants can reasonably claim as compensable expenses in this setting:**

> (A) **Seven (7) hours** between October 12 and October 24 for drafting letters, making phone calls, and engaging in negotiations (unjustifiably rendered fruitless by plaintiff and his counsel) to attempt to reduce the scope of and extend the time for the return on the subpoena (and to discuss terms of an appropriate protective order).

(B) **Twenty-five (25) hours** for researching and preparing the papers that defendants were constrained to submit in these proceedings (memoranda, declarations, and exhibits filed in connection with the emergency request for an order shortening time, the motion to quash, the amended notice and supplemental motion to quash, the separate motion for sanctions, and the replies to the oppositions to the motions).

(C) **Five (5) hours** for preparing for, traveling to and from, and attending the hearing on the motions.

The court further finds, based on its expertise and knowledge of fees in this area, declarations submitted, and the nature and quality of the papers filed, that $250 per hour is a reasonable blended rate for the compensable work performed by Mr. Idell and by Ms. Marone.

On these findings, the total sanction imposed for the violations described above is $9,250.00 (the product of multiplying 37 hours by $250 per hour).

It is hereby ORDERED THAT, BY MARCH 1, 2002:

a. **Iryna A. Kwasny pay defendants, through their counsel, the sum of $3,084.00.**

b. **Richard Metli pay defendants, through their counsel, the sum of $3, 084.00.**

c. **Alwyn V. H. Farey-Jones pay defendants, through their counsel, the sum of $3, 084.00.**

IT IS SO ORDERED.

Dated: February 1, 2002.

/s/
Wayne D. Brazil
United States Magistrate Judge

APPENDIX E

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

The Stored Communications Act, 18 U.S.C. §§ 2701 et seq.

Sec. 2701. - Unlawful access to stored communications

(a) Offense. -
Except as provided in subsection (c) of this section whoever -
(1)
intentionally accesses without authorization a facility through which an electronic communication service is provided; or
(2)
intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.
(b) Punishment. -
The punishment for an offense under subsection (a) of this section is -
(1)
if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain -
(A)
a fine under this title or imprisonment for not more than one year, or both, in the case of a first offense under this subparagraph; and

(B)

a fine under this title or imprisonment for not more than two years, or both, for any subsequent offense under this subparagraph; and

(2)

a fine under this title or imprisonment for not more than six months, or both, in any other case.

(c) Exceptions. -

Subsection (a) of this section does not apply with respect to conduct authorized -

(1)

by the person or entity providing a wire or electronic communications service;

(2)

by a user of that service with respect to a communication of or intended for that user; or

(3)

in section 2703, 2704 or 2518 of this title

Sec. 2702. - Voluntary disclosure of customer communications or records

(a) Prohibitions. -

Except as provided in subsection (b) -

(1)

a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service . . .

(2)

a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service -

(A)

on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;

(B)

solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and

Sec. 2703. - Required disclosure of customer communications or records

(b) Contents of Wire or Electronic Communications in a Remote Computing Service. -

(1)

A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection -

(A)

without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant; or

(B)

with prior notice from the governmental entity to the subscriber or customer if the governmental entity -

(i)

uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii)

obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

(2)

Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service -

(A)

on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B)

solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing

. . .

(e) No Cause of Action Against a Provider Disclosing Information Under This Chapter. -

No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, or certification under this chapter.

Sec. 2510. - Definitions

As used in this chapter - . . .

(17)
"electronic storage" means -
(A)
any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
(B)
any storage of such communication by an electronic communication service for purposes of backup protection of such communication; . . . .

Sec. 2707. - Civil action

(a) Cause of Action. -
Except as provided in section 2703(e), any provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

(b) Relief. -
In a civil action under this section, appropriate relief includes -
(1)
such preliminary and other equitable or declaratory relief as may be appropriate;
(2)
damages under subsection (c); and

(3)
a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) Damages. -
The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000. If the violation is willful or intentional, the court may assess punitive damages. In the case of a successful action to enforce liability under this section, the court may assess the costs of the action, together with reasonable attorney fees determined by the court.

. . .

(e) Defense. -

A good faith reliance on -
(1)
a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization (including a request of a governmental entity under section 2703 (f) of this title) . . . . is a complete defense to any civil or criminal action brought under this chapter or any other law.

Sec. 2711 - Definitions for chapter

As used in this chapter -
(1)
the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section;
. . .

APPENDIX F

No. 02-15742

IN THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

GEORGE THEOFEL, et. al.,
Plaintiffs-Appellants,

v.

ALWYN FAREY-JONES, et. al.,
Defendants-Appellees.

On Appeal from the United States District Court
for the Northern District of California

BRIEF FOR THE UNITED STATES AS AMICUS CURIAE SUPPORTING DEFENDANT/APPELLEE'S PETITION FOR REHEARING AND SUGGESTION FOR REHEARING EN BANC

CHRISTOPHER A. WRAY
Assistant Attorney General

MARK ECKENWILER
Deputy Chief
Computer Crime and Intellectual
Proptery Section

NATHAN JUDISH
Attorney, Computer Crime and
Intellectual Property Section
Criminal Division
U.S. Department of Justice
1301 New York Avenue, NW
Washington, D.C. 20530
(202)514-1026

TABLE OF CONTENTS

Page

INTRODUCTION AND STATEMENT OF INTEREST OF THE UNITED STATES OF AMERICA 1

STATEMENT OF FACTS 2

SUMMARY 4

ARGUMENT 6

- I. THE PANEL'S DECISION MISREADS THE DEFINITION OF "ELECTRONIC STORAGE" AND RENDERS SUPERFLUOUS KEY PORTIONS OF THE STORED COMMUNICATIONS ACT 6
  - A. The Panel's Interpretation of "Electronic Storage" Contradicts the Plain Language of the Statute 6
  - B. The Panel's Decision Threatens to Render Irrelevant Key Provisions of the Stored Communications Act 9
    - 1. The Panel's Decision Renders Superfluous the Statutorily Defined Term "Electronic Storage" 9
    - 2. The panel's broad interpretation of "electronic storage" renders § 2702(a)(2) and § 2703(b)

largely superfluous, and this interpretation creates an unprecedented impediment to law enforcement 11

    i. Under the panel's broad interpretation of "electronic storage," § 2702(a)(2) and § 2703(b) serve no practical function in the Stored Communications Act 11

    ii. The distinction between communications in "electronic storage" and other stored communications is critical to law enforcement 14

II. THE PANEL'S INTERPRETATION OF "ELECTRONIC STORAGE" CONFLICTS WITH THE STORED COMMUNICATIONS ACT'S LEGISLATIVE HISTORY 18

CONCLUSION 20

CERTIFICATE OF COMPLIANCE 21

CERTIFICATE OF SERVICE 22

TABLE OF AUTHORITIES

CASES

In re Doubleclick Inc. Privacy Litigation,
154 F. Supp. 2d 497 (S.D.N.Y. 2001) 14, 15

Fraser v. Nationwide. Mutual Insurance Co.,
135 F. Supp. 2d 623 (E.D. Pa. 2001) 14

Jones v United States,
529 U.S. 848 (2000) 15

Theofel v. Farey-Jones,
No. 02-15742 (9th Cir. Aug. 28, 2003) ..... passim

STATUTES and RULES

Stored Communications Act,
18 U.S.C. §§ 2701-2712 .... passim

USA Patriot Act, Pub. L. No. 107-56,
115 Stat. 272 (2001) 19

18 U.S.C. § 2510(17) .... passim

18 U.S.C. § 2702 .... passim

18 U.S.C. § 2703 .... passim

18 U.S.C. § 2707 15

18 U.S.C. § 2711 (2) 11

Fed. R. App. P. 29 1

MISCELLANEOUS

H.R. Rep. No. 236(I), 107th Cong., 1st Sess. (2001) . . 19

H.R. Rep. No. 647, 99th Cong., 2dSess. (1986) . . . 8, 18

H.R. Rep. No. 932, 106th Cong., 2nd Sess. (2000) . . . 19

Orin S. Kerr, A User's Guide to the Stored Communications Act-And A Legislator's Guide to Amending It, Geo. Wash. L. Rev. (forthcoming 2004) . 15

Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (2d ed. 2002) 15

INTRODUCTION AND STATEMENT OF INTEREST OF THE UNITED STATES OF AMERICA

The United States of America files this brief pursuant to Fed. R. App. P. 29.

This case, Theofel v. Farey-Jones, No. 02-15742 (9th Cir. Aug. 28, 2003), involves the construction of the term "electronic storage," 18 U.S.C. § 2510(17), which plays a key role in the Stored Communications Act, 18 U.S.C. §§ 2701-2712 ("SCA"). The panel's conclusion -- that e-mail messages remain in "electronic storage" regardless of whether they have been accessed by the addressee -- is contrary to the SCA's language, structure, and legislative history. Moreover, the panel's unprecedented interpretation of "electronic storage" upends the statutory framework for law enforcement's ability to compel disclosure of stored communications from network service providers, such as ISPs.

The panel's decision in Theofel largely nullifies 18 U.S.C. § 2703(b), the statutory provision of the SCA that governs law enforcement access to electronic communications not in "electronic storage." Federal prosecutors in the Ninth Circuit have ceased using § 2703(b) to compel disclosure of stored communications as a result of Theofel. Moreover, because the Internet spans state and national borders, the panel's decision is likely to create difficulties for law enforcement nationwide. For example, some of the nation's largest e-mail service providers, including Hotmail and Yahoo!, are located in the Ninth Circuit. Because such service providers must choose between compliance with § 2703(b) process issued elsewhere and adherence to the implications of Theofel, the panel's decision may upset criminal investigations across the United States.

In brief, because the panel's decision in this civil case has enormous implications in criminal law and procedure that the panel apparently did not recognize, the United States respectfully urges the court to grant the Petition for Rehearing and Suggestion for Rehearing En Banc of Defendant/Appellee Alwyn V. H. Farey-Jones (hereinafter "Petition for Rehearing").

STATEMENT OF FACTS

Theofel arose out of a discovery dispute in a separate commercial litigation involving at least two of the plaintiffs in Theofel and defendant Farey-Jones. In this separate litigation, Farey-Jones and his counsel subpoenaed an ISP which provided e-mail service to a corporation associated with the Theofel plaintiffs. The subpoena contained no limits based on time or scope. In response to the subpoena, the ISP copied 339 e-mail messages to a web site, and the messages were reviewed by Farey-Jones and his counsel. A magistrate subsequently quashed the subpoena, finding it "massively overbroad" and "patently unlawful." See Slip op. at 12338-39.

Following the quashing of the subpoena, the plaintiffs (all of whom had their e-mail viewed by the defendants) brought the instant suit seeking damages under the SCA, other federal statutes, and various state laws. Section 2707 of the SCA provides for a civil action against violators of the SCA's provisions. The plaintiffs alleged that the defendants violated § 2701 of the SCA, which provides for criminal penalties for one who "intentionally accesses without authorization a facility through which an electronic communication service is provided . . . and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage." 18 U.S.C. § 2701. The district court dismissed this claim.

The panel reversed. Only one issue addressed by the panel is of concern to the United States: whether the e-mail messages accessed by the defendants fell outside the scope of § 2701 because they were not "in electronic storage." Although the panel recognized that other courts have limited the definition of "electronic storage" to messages not yet delivered to their intended recipient, it asserted nevertheless that opened e-mails were "for purposes of backup protection" and thus fell within the scope of "electronic storage." Slip op. at 12345. The panel stated that "[a]n obvious purpose for storing a message on an ISP's server after delivery is to provide a second copy of the message in the event that the user needs to download it again-if, for example, the message is accidentally erased from the user's own computer. The ISP copy of the message functions as a 'backup' for the user." Id. The panel concluded that "plaintiffs' e-mail messages were in electronic storage regardless of whether they had been previously delivered." Id. at 12346.

SUMMARY

The Stored Communications Act, 18 U.S.C. §§ 2701-2712, sets forth a system of statutory privacy rights for customers and subscribers of computer network service providers. There are three main substantive components to this system, which serves to protect and regulate the privacy interests of network users with respect to government, network service providers, and the world at large. First, § 2703 regulates government access to stored communications. It creates a code of criminal procedure that federal and state law enforcement officers must follow to compel disclosure of stored communications. Second, § 2702 regulates voluntary disclosure by network service providers of customer communications and records, both to government and non-governmental entities. Third, § 2701 prohibits unlawful access to certain stored communications; anyone who obtains, alters, or prevents authorized access to those communications is subject to criminal penalties.

The structures of all three substantive components of the SCA reflect a series of classifications indicating congressional judgments about what kinds of information implicate greater or lesser privacy interests. In general, the SCA offers greater privacy protection to categories of information perceived by the SCA's drafters to implicate greater privacy interests. In setting forth this series of classifications, the SCA relies on a few key terms which are explicitly defined by statute. These terms are used throughout the SCA; a court's interpretation of a term for purposes of one provision of the SCA has important ramifications for the SCA's other provisions. One such term is "electronic storage," defined by 18 U.S.C. § 2510(17). The United States' interest in Theofel is limited to the interpretation of the scope of"electronic storage."

The panel's interpretation of "electronic storage" ignores the plain language of the term's definition, in particular that the "backup" subsection § 2510(17)(B) refers to backups of "temporary, intermediate" communications protected by § 2510(17)(A). The panel also ignored legislative history confirming this interpretation. Moreover, the panel's interpretation upsets the structure of the SCA, including the balance between § 2703(a) and § 2703(b), and in the process creates an unprecedented impediment for law enforcement access to stored communications. Because of the importance of this result for criminal investigations nationwide, the court should grant the Petition for Rehearing.

ARGUMENT

I. THE PANEL'S DECISION MISREADS THE DEFINITION OF "ELECTRONIC STORAGE" AND RENDERS SUPERFLUOUS KEY PORTIONS OF THE STORED COMMUNICATIONS ACT

A. The Panel's Interpretation of "Electronic Storage" Contradicts the Plain Language of the Statute.

"Electronic storage" is defined by statute to mean "(A) any temporary, immediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17). In Theofel, the panel held that "e-mail messages were in electronic storage regardless of whether they had been previously delivered." Slip op. at 12346. The panel did not dispute that delivered e-mail did not fit "within the purview of subsection (A)," because delivered e-mail is not in "temporary, intermediate" storage. Slip op. at 12345. However, the panel incorrectly held that delivered e-mail fell within the scope of § 2510(17)(B) because messages remain stored on the ISP as a "backup" for the user. Slip op. at 12345.

The holding that e-mail that has been delivered remains in "electronic storage" conflicts with the plain language of the Stored Communications Act ("SCA"). As an initial matter, the panel treated the "backup" subsection of the definition (§ 2510(17)(B)) as independent of the "temporary, intermediate" subsection (§ 2510(17)(A)). The panel noted that "[a]n obvious purpose for storing a message on an ISP's server after delivery is to provide a second copy of the message in the event that the user needs to download it again-if, for example, the message is accidentally erased from the user's own computer." Slip op. at 12345. The panel concluded that storage of delivered e-mail fell "literally" within the scope of "electronic storage." Id. However, § 2510(17)(B) refers to "any storage of such communication by an electronic communication service for purposes of backup protection of such communication" (emphasis added). The phrase "such communication" necessarily refers to the communications defined in subsection § 2510(17)(A): communications stored temporarily at an intermediate point in transmission. **Therefore § 2510(17)(B) can encompass only backup copies of communications which are themselves in temporary, intermediate storage incidental to transmission.**

In support of its contrary conclusion, the panel mistakenly asserted that a narrow interpretation of "electronic storage" would render § 2510(17)(B) superfluous. See Slip op. at 12346. This erroneous claim is based on the assumption that under the narrow interpretation of "electronic storage," backups must also be temporary. The panel asserted that "Fraser's [narrow] interpretation [of electronic storage] renders subsection (B) essentially superfluous, since temporary backup storage pending transmission would already seem to qualify as 'temporary, intermediate storage' within the meaning of subsection (A)." Slip op. at 12346 (emphasis added). However, under the plain language of § 2510(17)(B), the backup itself need not be temporary: what is essential is that the underlying communication be in temporary, intermediate storage. Thus, the panel grafted on an additional requirement (that backups be temporary) to the narrow meaning of § 2510(17)(B). Without this novel addition,

§ 2510(17)(B) is not superfluous under the narrow meaning of "electronic storage."

In this context, it is useful to consider what the term "backup" meant to the drafters of the SCA. In 1986, providers of electronic communication service commonly stored copies of files to protect against system failure. For example, the House Report on the SCA states that "[b]ack up protection preserves the integrity of the electronic communications system and to some extent preserves the property of users of such a system." H.R. Rep. No. 647, 99th Cong., 2d Sess., at 68 (1986). By including backup protections within the definition of "electronic storage," Congress ensured that backups would receive the same degree of protection as the underlying communications.

B. The Panel's Decision Threatens to Render Irrelevant Key Provisions of the Stored Communications Act

The structure of the SCA further demonstrates that "electronic storage" should not be given the expansive definition provided by Theofel. First, the panel's broad reading of "electronic storage" would render that statutorily defined term itself superfluous throughout the SCA. Second, the panel's broad interpretation of "electronic storage" also renders § 2702(a)(2) and § 2703(b) largely superfluous.

1. The Panel's Decision Renders Superfluous the Statutorily Defined Term "Electronic Storage"

Under Theofel, a backup falls within § 2510(17)(B) if it provides backup protection for either a user or a service provider. See Slip op. at 12345. Under this interpretation, any communication stored by an electronic communication service will be in "electronic storage." If a communication is in temporary, intermediate storage incident to transmission, it will fall under § 2510(17)(A). Any other copy of the communication stored by an electronic communication service will necessarily serve as a backup to either the user, the service, or both. Thus, any other copy will fall under § 2510(17)(B).

The defect in this reasoning is clear. If, as Theofel implies, any communication stored by an electronic communication service is in "electronic storage," the term "electronic storage" becomes mere surplusage. In the SCA, the term "electronic storage" appears only in the following locations:

- § 2701 (a) prohibits unauthorized access "to a wire or electronic communication while it is in electronic storage" in an electronic communication service (emphasis added).

- § 2702(a)(1) prohibits a provider of electronic communication service to the public from disclosing "the contents of a communication while in electronic storage"(emphasis added).

- § 2703(a) sets rules under which the government may compel a provider of electronic communication service to disclose either (1) "the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less" (emphasis added) or (2) "the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days" (emphasis added).

In each of these sections, the underlined language is superfluous under the panel's decision.

2. The panel's broad interpretation of "electronic storage" renders § 2702(a)(2) and § 2703(b) largely superfluous, and this interpretation creates an unprecedented impediment to law enforcement

Far more importantly, the panel's decision effectively obliterates the SCA's essential distinction between two categories of communications: (1) electronic communications in "electronic storage" in an "electronic communication service" and (2) electronic communications stored by a "remote computing service." [1] As explained below, under Theofel, the former would swallow the latter.

i. Under the panel's broad interpretation of "electronic storage," § 2702(a)(2) and § 2703(b) serve no practical function in the Stored Communications Act

The dichotomy between communications in "electronic storage" and those not in "electronic storage" permeates the SCA. In adopting an overbroad reading of this defined term, the panel effectively eliminated this distinction.

---

[1] The term "remote computing service" is defined by 18 U.S.C. § 2711(2) as "provision to the public of computer storage or processing services by means of an electronic communications system."

For example, § 2703, which controls government access to stored communications, provides greater protection to communications in "electronic storage" than to other stored communications. Section 2703(a) provides that "[a] government entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communication system for one hundred and eighty days or less, only pursuant to a warrant . . ." (emphasis added). Thus, law enforcement can generally compel disclosures of e-mail "in electronic storage" only upon a showing of probable cause.[2]

In contrast, § 2703(b)(1)(B) allows law enforcement to compel a provider of "remote computing service" to disclose the contents of an electronic communication by means of a subpoena or a court order under 18 U.S.C. § 2703(d).[3] Thus, prosecutors can obtain access to files stored with a remote computing service using a standard lower than probable cause.[4]

---

[2] E-mail in "electronic storage" more than 180 days can be obtained by the government pursuant to a subpoena or 2703(d) order. See 18 U.S.C. § 2703(a) (stating that such communications can be compelled "by the means available under subsection (b) of this section").

[3] A 2703(d) order requires the government to offer "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).

[4] Prosecutors retain the option of using a § 2703(a) search

This dichotomy between communications in "electronic storage" and other communications is mirrored in the SCA's rules relating to voluntary (not compulsory) disclosure of communications by network service providers. Under § 2702(a)(1), providers of electronic communication service are generally prohibited from voluntarily disclosing user communications in "electronic storage." Providers of remote computing service - often the same entities - are prohibited by § 2702(a)(2) from voluntarily disclosing other user communications.

The communications governed by the precisely parallel non-"electronic storage" provisions, §§ 2702(a)(2) and 2703(b), are subject to additional (and identical) limitations. Each of these provisions applies explicitly to communications held by a service provider "solely for the purpose of providing storage or computer processing services to [the] subscriber or customer." § 2702(a)(2)(B); § 2703(b)(2)(B)(emphasis added). Plainly, communications within this category are not in "electronic storage," which is dealt with in parallel subsections (§§ 2702(a)(1) and 2703(a)), or these references to "providing storage . . . to [the] subscriber" would be utterly superfluous. Yet the panel's decision declares that such convenience storage is a "backup" (and therefore within the meaning of "electronic storage"), abolishing a distinction written expressly into the Act. Such an interpretation renders largely superfluous § 2702(a)(2) and § 2703(b).

---

warrant to compel production of electronic communications stored by a remote computing service. See 18 U.S.C. § 2703(b)(1)(A).

ii. The distinction between communications in "electronic storage" and other stored communications is critical to law enforcement

The distinction between electronic communications in "electronic storage" and subject to the requirements of § 2703(a) and other electronic communications subject to § 2703(b) is critical for law enforcement, because § 2703 places greater restrictions on government access to communications in electronic storage. As traditionally understood by Congress, other courts, and the Department of Justice, the term "electronic storage" is much more limited than its everyday meaning. Under this traditional interpretation, "electronic storage" refers only to temporary storage, made in the course of transmission, by a provider of electronic communications service, and to backups of such intermediate communications. See Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp.2d 623,636 (E.D. Pa. 2001) (stating that "[t]he phrase 'for purposes of backup protection of such communication' in the statutory definition makes clear that messages that are in post-transmission storage, after transmission is complete, are not covered by part (B) of the definition of 'electronic storage'"); In re Doubleclick Inc. Privacy Litigation, 154 F. Supp.2d 497, 511-13 (S.D.N.Y. 2001) (emphasizing that "electronic storage" should have a narrow interpretation based on statutory interpretation and legislative intent)[5]; Searching and Seizing Computers and

---

[5] In interpreting the term "electronic storage" narrowly, the Doubleclick court also relied upon the canon of statutory interpretation which disfavors a broad reading of a criminal statute. See Doubleclick, 154 F. Supp.2d at 513. That rule is equally applicable to Theofel. Although Theofel is a civil suit under § 2707 of the SCA, civil liability under § 2707 for a violation of § 2701 is coextensive with criminal liability under § 2701. Because Theofel

Obtaining Electronic Evidence in Criminal Investigations 86-87 (2d ed. 2002), available at http://www.cybercrime.gov/s&smanual2002.pdf.

Under this narrow interpretation of"electronic storage," a copy of an e-mail is in "electronic storage" only if it is at an intermediate point in its transmission and has not yet been sent on to its final destination, the recipient of the e-mail. If an e-mail has been received by a recipient's ISP but has not yet been accessed by the recipient, it is in "electronic storage." Once the recipient retrieves the e-mail, however, the communication reaches its final destination. If the recipient chooses to retain a copy of the e-mail on the ISP's system, the copy on the network is no longer in "electronic storage" because it is no longer in "temporary, intermediate storage . . . incidental to. . . electronic transmission." See Orin S. Kerr, A User's Guide to the Stored Communications Act-And A Legislator's Guide to Amending It, Geo. Wash. L. Rev. (forthcoming 2004), available at http:\\papers.ssm.corn/so13/papers.cfm?abstract_id=421860, at 7-8 (draft).

Even under this traditional interpretation of "electronic storage," opened and retained e-mail stored with an ISP is not without protection under the SCA. However, its categorization under the SCA changes once a copy is delivered to its intended recipient, and it receives somewhat less privacy protection. Such e-mail retained on the provider's system is no longer an "electronic communication . . . in

---

reads "electronic storage" expansively, it also reads criminal liability under § 2701 expansively, contrary to the canons of statutory interpretation. See Jones v. United States, 529 U.S. 848, 858 (2000).

electronic storage;" instead, it becomes an electronic communication stored by a "remote computing service." See id.

Combining the structure of § 2703(a) and (b) with the traditional interpretation of the status of e-mail under the SCA yields the following framework for compelling disclosure of e-mail, which until now has been followed by federal prosecutors nationwide:

- Unopened e-mail stored on an ISP's servers constitutes electronic communications in electronic storage. Such e-mail can be obtained only using a warrant based on probable cause, unless it is more than 180 days old.

- Opened e-mail or copies of sent e-mail retained by users constitute files stored with a remote computing service. Such files can be obtainedpursuant to § 2703(b)(1)(B) using a subpoena or 2703(d) order, or pursuant to § 2703(b)(1)(A) using a warrant based on probable cause.

Theofel overturns this framework. Under Theofel, all copies of e-mail stored by a network services provider constitute electronic communications in electronic storage and hence are available to law enforcement only pursuant to a warrant based on probable cause, unless they are more than 180 days old. Substantial quantities of evidence previously available to state and federal prosecutors are no longer available under this heightened standard. Such evidence is often critical in a broad spectrum of cases, including cases involving network intrusion, fraud, child pornography, and illegal drugs. The significance of this change for law enforcement cannot be overstated.

In addition, because the Internet spans state borders, Theofel is likely to create conflicts for law enforcement nationwide. Network service providers who violate the SCA are subject to civil suit under § 2707. They may face civil suits in the Ninth Circuit for responding to government process under § 2703(b) from outside the Ninth Circuit. Such suits are particularly likely to be a problem for service providers located in the Ninth Circuit, like Hotmail and Yahoo!. Alternatively, network service providers outside the Ninth Circuit may fear lawsuits brought by customers within the Ninth Circuit. Network service providers may begin to resist subpoenas and 2703(d) orders under § 2703(b), even when that process does not come from the Ninth Circuit. Thus, Theofel will likely prove disruptive for law enforcement nationwide.

II. THE PANEL'S INTERPRETATION OF "ELECTRONIC STORAGE" CONFLICTS WITH THE STORED COMMUNICATIONS ACT'S LEGISLATIVE HISTORY

The error in the panel's holding - that e-mail is in "electronic storage" regardless of whether it has been delivered - is further confirmed by the SCA's legislative history. As explained below, Congress intended a much narrower reading of "electronic storage." For that reason, the Petition for Rehearing should be granted.

In the course of considering the SCA's prohibitions on voluntary disclosure by network service providers of customer communications, the drafters of the SCA in 1986 explicitly considered what would happen when a recipient of e-mail kept a copy of the e-mail on his ISP after receipt:

> Sometimes the addressee, having requested and received a message, chooses to leave it in storage on the service for re-access at a later time. The Committee intends that, in leaving the message in storage, the addressee should be considered the subscriber or user from whom the system received the communication for storage, and that such communication should continue to be covered by section 2702(a)(2).

H.R. Rep. No. 647, 99th Cong., 2nd Sess., at 65 (1986) (emphasis added). As explained above, § 2702(a)(2) prohibits disclosure of communications stored by a remote computing service, rather than communications in "electronic storage" in an electronic communication service (which are covered by § 2702(a)(1)). The House Report in effect says the following: when a customer opens an e-mail message and leaves a copy on the ISP server, the copy is treated as a communication maintained by a remote computing service.

Subsequent legislative history confirms Congress's continued understanding that previously delivered e-mail maintained by an ISP is not in electronic storage. In 2000, Congress considered and rejected amending the definition of electronic storage to include "any storage of an electronic communication by an electronic communication service without regard to whether the communication has been accessed by the intended recipient." See H.R. Rep. No. 932, 106th Cong., 2nd Sess. at 7 (2000) (emphasis added). The drafters of this amendment understood that previously accessed e-mail did not fall within the scope of § 2510(17).

In addition, the House Report on the USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 272 (2001), demonstrated Congress's narrow understanding of the term "electronic storage." In the course of discussing an amendment to the SCA allowing for nationwide service of § 2703(a) warrants, the Report states that "2703(a) requires a search warrant to compel service providers to disclose unopened e-mails." H.R. Rep. No. 236(I), 107th Cong., 1st Sess. at 57 (2001) (emphasis added). Because warrants under § 2703(a) are required only for electronic communications in "electronic storage," this statement is further evidence that Congress did not intend opened e-mail to fall within the scope of "electronic storage." The panel has supplied the term "electronic storage" with a meaning rejected by Congress, thereby creating difficulties for law enforcement. Therefore, the Petition for Rehearing should be granted.

CONCLUSION

For the foregoing reasons, this Court should grant the Petition for Rehearing.

Respectfully submitted.

CHRISTOPHER A. WRAY
Assistant Attorney General

/s/
MARK ECKENWILER
Deputy Chief
Computer Crime and Intellectual Property Section

NATHAN JUDISH
Attorney, Computer Crime and Intellectual Property Section
Criminal Division
U.S. Department of Justice
Washington, D.C. 20530

CERTIFICATE OF COMPLIANCE

I certify that pursuant to Circuit Rules 35-4 and 40-1 the attached Brief for the United States as Amicus Curiae Supporting Defendant/Appellee's Petition for Rehearing and Suggestion for Rehearing En Banc is proportionately spaced, has a typeface of 14 points, and contains 4136 words as counted by the word processing system on which it was prepared.

/s/
Mark Eckenwiler

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that two copies of the foregoing Brief for the United States as Amicus Curiae Supporting Defendant/Appellee's Petition for Rehearing and Suggestion for Rehearing En Banc were this day sent by regular mail to the following person(s):

Robert E White
Susan C. Rushakoff
Law Offices of Robert E. White
177 Post Street, Suite 890
San Francisco, CA 94108

James M. Wagstaffe
Pamela Urueta
Kerr & Wagstaffe LLP
100 Spear Street, Suite 1800
San Francisco, CA 94105

Richard Idell
Jennifer Marone
Idell, Berman & Seitel
530 Bush Street, Suite 601
San Francisco, CA 94105

Iryna A. Kwasny
Environmental Law Foundation
1736 Franklin Street, 9th Floor
Oakland, CA 94612

/s

MARK ECKENWILER
Deputy Chief
U.S. Department of Justice Criminal Division
Computer Crime and Intellectual Property Section
1301 New York Avenue. NW Suite 600
Washington, D.C. 20530
(202) 514-1026

Dated: SEPTEMBER 25, 2003